CISCO SYSTEMS

Cisco IP Phone Models 7905G and 7912G Administrator Guide (SIP)

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-4277-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Cisco IP Phone Models 7905G and 7912G Administrator Guide (SIP)
Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Preface xi

Overview xi

Audience xi

Organization xii

Related Documentation xiii

Obtaining Documentation xiii

World Wide Web xiii

Documentation CD-ROM xiii

Ordering Documentation xiv

Documentation Feedback xiv

Obtaining Technical Assistance xiv

Cisco Connection Online xv

Technical Assistance Center xv

Obtaining Additional Publications and Information xvi

Document Conventions xvii

CHAPTER 1 **Overview of the Cisco IP Phone Models 7905G and 7912G** 1-1

Hardware Overview 1-1

Software Features 1-4

Protocols 1-4

Basic Services 1-5

Supplemental Services 1-5

SIP-Specific Services 1-6

SIP Overview 1-7
SIP Functions 1-7
SIP Components 1-8

CHAPTER 2 **Installing the Cisco IP Phone Models 7905G and 7912G 2-1**
Prerequisites 2-1
Safety 2-2
Connecting to the Network 2-4
Providing Power to the Cisco IP Phone 2-5
Power Source Design 2-5
Redundancy Feature 2-6
Installing the Cisco IP Phone Models 7905G and 7912G 2-6
Physical Installation of the Cisco IP Phone Models 7905G and 7912G 2-7
Mounting the Phone to the Wall 2-12
Basic Configuration of the Cisco IP Phone Models 7905G and 7912G 2-13
Verifying Installation 2-15

CHAPTER 3 **Configuring the Cisco IP Phone Models 7905G and 7912G for SIP 3-1**
Overview of Configuration Methods 3-1
Default Boot Load Behavior 3-2
Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation 3-4
Basic Configuration Steps in a TFTP Server Environment 3-6
Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G 3-9
Making Settings with a DHCP Server 3-9
Making Settings Manually 3-10

CHAPTER 4 **Basic and Additional SIP Services** 4-1

Important Basic SIP Services 4-2

Required Parameters 4-2

Establishing Authentication 4-4

Configuring Refresh Interval 4-4

Additional SIP Services 4-4

Setting Up and Placing a Call Without Using a SIP Proxy 4-10

Complete Reference of all Cisco IP Phone SIP Services 4-12

CHAPTER 5 **Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus** 5-1

Configuration Menus on the Cisco IP Phone 5-2

Displaying a Configuration Menu 5-3

Unlocking and Locking Configuration Parameters 5-4

Editing Parameter Values 5-5

Network Configuration Menu 5-6

SIP Configuration Menu 5-14

Model Information Menu 5-17

Status Menu 5-18

CHAPTER 6 **Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server** 6-1

Using Profiles with TFTP Configuration 6-2

Setting Up the TFTP Server with Cisco IP Phone Software 6-4

Configuring the Cisco IP Phone to Obtain its Configuration File from the TFTP Server 6-5

Using a DHCP Server 6-5

Without Using a DHCP Server 6-8

Creating or Updating a Profile 6-9
Profile Conventions 6-10
Creating a Phone-Specific Profile 6-11
Creating a Default Profile 6-13
Using Encryption 6-15
Refreshing or Resetting the Cisco IP Phone 6-17
Refreshing the Cisco IP Phone 6-17
Resetting the Cisco IP Phone 6-17

CHAPTER 7 **Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages 7-1**
Accessing a Phone's Web Page 7-2
Viewing Statistical and Operational Information 7-4
Device Information 7-4
Network Configuration 7-5
Network Statistics 7-6

CHAPTER 8 **Profile and Web Page Parameters and Defaults 8-1**
Network Parameters 8-2
SIP Parameters 8-9
Call Preference Parameters 8-13
Tone Parameters 8-21
Audio Parameters 8-24
Profile Parameters 8-26
Parameter Details 8-27
BusyTone, CallWaitTone, DialTone, DialTone2, and RingBackTone Parameter Details 8-28
ReorderTone Parameter Details 8-30
ConnectMode Detail 8-36

DialPlan Parameter Detail 8-38
Upgradecode Parameter Detail 8-41
Upgradelogo Parameter Detail 8-43

CHAPTER 9 **Troubleshooting the Cisco IP Phone Models 7905G and 7912G** 9-1
General Troubleshooting Tips 9-1
Resolving Problems 9-2
Contacting TAC 9-5
Debugging 9-5

APPENDIX A **Additional End User Features on the Cisco IP Phone Models 7905G and 7912G** A-1
Call Preferences Menu A-1
Softkeys A-6
Other Features A-7

APPENDIX B **Phone Menu, Web Page, and Profile Equivalent Parameters** B-1

APPENDIX C **SIP Call Flows** C-1
Supported SIP Request Methods C-1
Call Flow Scenarios for Successful Calls C-2
Cisco IP Phone-to-SIP Server—Registration without Authentication C-2
Cisco IP Phone-to-SIP Server—Registration with Authentication C-4
Cisco IP Phone-to-Cisco IP Phone—Basic SIP to SIP Call without Authentication C-7
Cisco IP Phone-to-Cisco IP Phone—Basic SIP to SIP Call with Authentication C-15

APPENDIX D **Specifications for the Cisco IP Phone Models 7905G and 7912G** **D-1**

Physical Specifications **D-2**

Electrical Specifications **D-2**

Environmental Specifications **D-3**

Physical Interfaces **D-3**

Software Specifications **D-3**

GLOSSARY

INDEX

Preface

Overview

Cisco IP Phone Models 7905G and 7912G Administrator Guide (SIP) describes how to install and configure the Cisco IP Phone models 7905G and 7912G for use on a Session Initiation protocol (SIP) network. It includes configuration steps for network parameters, standard services, and supplemental services.

This guide does not cover information that is related to the implementation of a SIP Voice over IP (VoIP) network.

Audience

This guide is intended for service providers and network administrators who administer VoIP services using the Cisco IP Phone models 7905G and 7912G and who have a fundamental understanding of SIP. The tasks described in this guide are not intended for end users of the phones. Many of these tasks affect the ability of a phone to function on the network and require an understanding of IP networking and telephony concepts.

Organization

This manual is organized as follows:

Chapter 1, “Overview of the Cisco IP Phone Models 7905G and 7912G”	Describes the hardware and software features of the phone and provides a brief overview of SIP
Chapter 2, “Installing the Cisco IP Phone Models 7905G and 7912G”	Provides procedures for installing the phone at an end user location
Chapter 3, “Configuring the Cisco IP Phone Models 7905G and 7912G for SIP”	Provides an overview of how to configure the phone to operate with the SIP signaling image
Chapter 4, “Basic and Additional SIP Services”	Provides information about basic and additional SIP services that the phone supports
Chapter 5, “Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus”	Explains how to use menus on the phone to configure or view a variety of network, SIP, and phone settings
Chapter 6, “Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server”	Explains how to configure a phone using a Trivial File Transfer Protocol (TFTP) server
Chapter 7, “Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages”	Describes how to use a phone’s web page to configure parameters and obtain information
Chapter 8, “Profile and Web Page Parameters and Defaults”	Describes the parameters that you can use to configure a phone through a profile or through a phone’s web page
Chapter 9, “Troubleshooting the Cisco IP Phone Models 7905G and 7912G”	Provides guidance for diagnosing and correcting installation and configuration errors
Appendix A, “Additional End User Features on the Cisco IP Phone Models 7905G and 7912G”	Describes end-user features that are not explained in the User Guide for the phone
Appendix B, “Phone Menu, Web Page, and Profile Equivalent Parameters”	Lists the configurable options on the phone menus and their equivalent parameters in the phone configuration web pages and profile
Appendix C, “SIP Call Flows”	Describes some basic call flows for the phone

Appendix D, “Specifications for the Cisco IP Phone Models 7905G and 7912G”	Provides physical, electrical, environmental, and software specifications for the phone
Glossary	Explains terms that may be new to you

Related Documentation

For more information, refer to the following documents, which are available at this URL:

http://www.cisco.com/en/US/products/hw/phones/index.html

- *Cisco IP Phone 7905G/7912G User Guide for Cisco CallManager*
- *Regulatory Compliance and Safety Information for the Cisco IP Phone 7900 Series*

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.

Convention	Description
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告　重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告　安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

Overview of the Cisco IP Phone Models 7905G and 7912G

This chapter describes the hardware and software features of the Cisco IP Phone models 7905G and 7912G and provides a brief overview of the Session Initiation Protocol (SIP).

This chapter includes the following sections:

- Hardware Overview, page 1-1
- Software Features, page 1-4
- SIP Overview, page 1-7

Hardware Overview

The Cisco IP Phone models 7905G and 7912G are cost-effective, entry-level, single-line telephones that operate on IP-based telephony networks. They can function as desk units or be mounted on a wall. The phones are easily installed by end-users.

Figure 1-1 shows the main components of the Cisco IP Phone models 7905G and 7912G.

Figure 1-1 Cisco IP Phone Models 7905G and 7912G Features

1	LCD screen	Displays features such as the time, date, your phone number, caller ID, call status, and softkey tabs.
2	Cisco IP Phone series type	Indicates the Cisco IP Phone series to which the phone belongs.
3	Softkeys	Enable you to engage any of the functions displayed on the corresponding LCD screen tabs. Softkeys point to feature options displayed along the bottom of the LCD screen. Softkey functions change depending on the status of your phone (for example, if the phone is active or idle).

4	Navigation button	Enables you to scroll through text and select features displayed on the LCD screen. Also provides access to speed dial numbers when there are no text or features to scroll through.
5	Menu button	Provides access to phone services and settings such as messages, directories, contrast, ring sound, network configuration, and status information.
6	Hold button	Puts a current call on hold or takes a call off hold.
7	Dial pad	Works exactly like the dial pad on a traditional telephone.
8	Volume button	Increases or decreases volume for the handset and speaker. Also controls the ringer volume (if on-hook).
9	Handset	Functions like a traditional handset. The light strip at the top of the handset blinks when the phone rings and remains lit to indicate a new voice mail message (depending on your message system).
10	Footstand	Allows the phone to stand at a convenient angle on a desk or table.

Software Features

The Cisco IP Phone models 7905G and 7912G support the following software features:

- Protocols, page 1-4
- Basic Services, page 1-5
- Supplemental Services, page 1-5
- SIP-Specific Services, page 1-6

Protocols

The Cisco IP Phone models 7905G and 7912G support the following protocols:

- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Internet Control Message Protocol (ICMP)
- Internet Protocol (IP)
- Network Time Protocol (NTP)
- Real-Time Transport Protocol (RTP)
- Session Initiation Protocol (SIP)
- Transmission Control Protocol (TCP)
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)

Related Topics

- Basic Services, page 1-5
- Supplemental Services, page 1-5
- SIP-Specific Services, page 1-6

Basic Services

The Cisco IP Phone models 7905G and 7912G provide the following basic services:

- Configuration using LCD screen menus, TFTP server, or web browser
- IP address assignment—DHCP or manual static IP address
- Configurable Type of Service (ToS) bit for Quality of Service (QoS)
- Configurable tone (busy tone, call waiting tone, dial tone, secondary dial tone, reorder tone, ringback tone)
- Dial plan support
- Remote reset support
- G.711 u-law, G.711 A-law, and G.729A support
- Voice-activity-detection (VAD) and comfort-noise-generation (CNG) support for G.711 u-law and G.711 A-law, and support for G.729 Annex B
- Dynamic jitter buffer for voice packets

Related Topics

- Protocols, page 1-4
- Supplemental Services, page 1-5
- SIP-Specific Services, page 1-6

Supplemental Services

The Cisco IP Phone models 7905G and 7912G support the following supplemental services:

- Call waiting
- Calling line ID presentation/rejection (CLIP/CLIR)
- Three-way calling
- Conferencing bridge—up to three parties
- Call hold

- Call transfer—attended and unattended
- Message-waiting indicator

Related Topics

- Protocols, page 1-4
- Basic Services, page 1-5
- SIP-Specific Services, page 1-6

SIP-Specific Services

The Cisco IP Phone models 7905G and 7912G support the following SIP-specific services:

- Direct IP dialing in addition to proxy-routed calls.
- Configurable periodic registration with a SIP proxy server.
- Authentication support for all SIP methods.
- Configurable NAT support.
- Configurable outbound proxy support.
- Local support for call return (or call back), call forwarding, and call transfer.
- FQDN for SIP proxy and outbound proxy.
- Uses the same configurable MediaPort to transmit and receive RTP audio.
- Out-of-Band DTMF via RFC2833 (also known as AVT tones).
- UDP for SIP signaling.
- Message-waiting indication (MWI) provided via the telephone-handset LED lamp.
- Distinctive ringing support via the SIP Alert-Info header.

Related Topics

- Protocols, page 1-4
- Basic Services, page 1-5
- Supplemental Services, page 1-5

SIP Overview

Session Initiation Protocol (SIP) is the Internet Engineering Task Force (IETF) standard for real-time calls and conferencing over Internet Protocol (IP). SIP is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate calls between two or more endpoints.

Like other VoIP protocols, SIP provides signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management controls the attributes of an end-to-end call.

This section includes these topics:

- SIP Functions, page 1-7
- SIP Components, page 1-8

SIP Functions

SIP does the following:

- Determines the location of the target endpoint—SIP supports address resolution, name mapping, and call redirection.
- Determines the media capabilities of the target endpoint—Via Session Description Protocol (SDP), SIP determines the lowest level of common services between endpoints. Conferences are established using only the media capabilities that can be supported by all endpoints.
- Determines the availability of the target endpoint—If a call cannot be completed because the target endpoint is unavailable, SIP determines whether the called party is already on the phone or did not answer in the allotted number of rings. It then returns a message indicating why the target endpoint was unavailable.
- Establishes a session between the originating and target endpoint—If the call can be completed, SIP establishes a session between the endpoints. SIP also supports mid-call changes such as adding another endpoint to the conference and changing media characteristic or codec.
- Transfers and terminates calls—SIP supports the transfer of calls from one endpoint to another. During call transfer, SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring

party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates sessions between all parties. Conferences can consist of two or more users and can be established using multicast or multiple unicast sessions.

Related Topic

- SIP Components, page 1-8

SIP Components

SIP is a peer-to-peer protocol. The peers in a session are called user agents (UAs). A user agent can function in either of two roles:

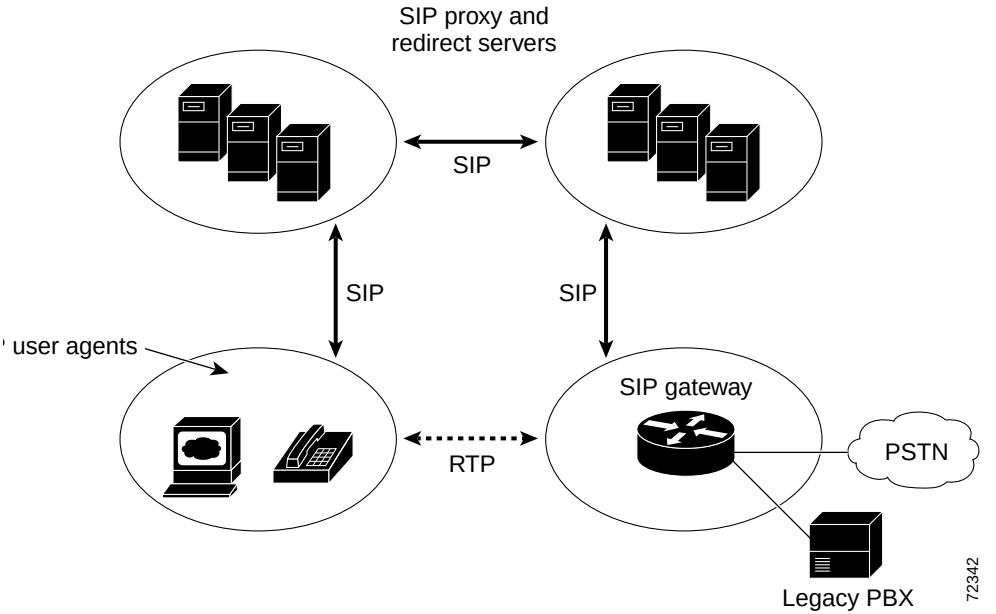
- User-agent client (UAC)—A client application that initiates the SIP request.
- User-agent server (UAS)—A server application that contacts the user when a SIP request is received and returns a response on behalf of the user.

  SIP servers can interact with other back-end application services such as Lightweight Directory Access Protocol (LDAP) servers, database applications, and extensible markup language (XML) applications that provide back-end services such as directory, authentication, and billing services.

Typically, a SIP endpoint is capable of functioning as either UAC or UAS (but not both simultaneously) during a transaction. Whether it functions as UAC or UAS depends on the UA that initiated the request.

Figure 1-2 shows the architecture of a SIP network.

Figure 1-2 SIP Architecture



Related Topic

- SIP Functions, page 1-7
- SIP Clients, page 1-9
- SIP Servers, page 1-10

SIP Clients

SIP clients include the following:

- Telephones—Act as either UAS or UAC. The Cisco IP Phone models 7905G and 7912G can initiate SIP requests and respond to requests.
- Gateways—Provide call control. Gateways provide many services, the most common being translation between SIP conferencing endpoints of transmission format, communications procedures, and codecs. Other functions include call setup and clearing on both the LAN side and the switched-circuit network side.

SIP Servers

SIP servers include the following:

- Proxy servers—Receive SIP requests from a client and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
- Redirect servers—Receive SIP requests, strip out the address in the request, check its address tables for any other addresses that may be mapped to the one in the request, and return the results of the address mapping to the client. Basically, redirect servers provide the client with information about the next one or more hops that a message should take and then the client contacts the next hop server or UAS directly.
- Registrar servers—Process requests from UACs for registration of their current location. Registrar servers are often colocated with redirect or proxy servers.

Installing the Cisco IP Phone Models 7905G and 7912G

This chapter provides information about installing the Cisco IP Phone models 7905G and 7912G at the end user location. It includes the following sections:

- Prerequisites, page 2-1
- Safety, page 2-2
- Connecting to the Network, page 2-4
- Providing Power to the Cisco IP Phone, page 2-5
- Installing the Cisco IP Phone Models 7905G and 7912G, page 2-6
- Verifying Installation, page 2-15

Prerequisites

The Cisco IP Phone models 7905G and 7912G act as endpoints on an IP telephony network, and have the following network requirements:

- An Ethernet connection to a network with SIP clients and servers, as required
- A Trivial File Transfer Protocol (TFTP) server for storing IP phone profiles, if desired
- A Dynamic Host Configuration Protocol (DHCP) server, if desired

- A Call Control System
  - Proxy server—There must be a device running RFC 2543 SIP-compliant software
  - Voice packet gateway—Required if you are connecting to the Public Switched Telephone Network (PSTN)

Note If you use a firewall, Cisco recommends that it be a Cisco PIX firewall, Version 5 or later.

Related Topics

- Safety, page 2-2
- Connecting to the Network, page 2-4
- Providing Power to the Cisco IP Phone, page 2-5
- Installing the Cisco IP Phone Models 7905G and 7912G, page 2-6
- Verifying Installation, page 2-15

Safety

To ensure general safety, follow these guidelines:

- Do not open or disassemble this product.
- Do not get this product wet or pour liquids into this device.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.**

Warning **Read the installation instructions before you connect the system to its power source. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.**

Warning **The plug-socket combination must be accessible at all times because it serves as the main disconnecting device. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.**

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.**

Warning **This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors). To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.**

Warning **The device is designed to work with TN power systems. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.**

Related Topics

- Connecting to the Network, page 2-4
- Providing Power to the Cisco IP Phone, page 2-5
- Installing the Cisco IP Phone Models 7905G and 7912G, page 2-6
- Verifying Installation, page 2-15

Connecting to the Network

The Cisco IP Phone 7912G has two RJ-45 ports labelled “10/100 SW” and “10/100 PC.” Each port supports 10/100 Mbps half- or full-duplex connections to external devices. The Cisco IP Phone 7905G has one RJ-45 port labeled “10 BASET.” This port supports 10 Mbps half- or full-duplex connections to external devices. You can use Category 3 or 5 cabling for 10-Mbps connections, but you must use Category 5 cabling for 100 Mbps connections. Cisco recommends that you use full-duplex mode on all ports (set at the switch) to avoid collisions.

Use the 10BASET port on the Cisco IP Phone 7905G or the 10/100 SW port on the Cisco IP Phone 7912G to connect a phone to the network. You must use a straight-through cable on these ports. A phone can also obtain inline power over these connections.

Use the 10/100 PC port on the Cisco IP Phone 7912G to connect a network device, such as a computer, to the phone. You must use a straight-through cable on this port.

Figure 2-1 shows the connection ports on the back of the Cisco IP Phone 7905G. Figure 2-2 shows the connection ports on the back of the Cisco IP Phone 7912G.

Related Topics

- Safety, page 2-2
- Providing Power to the Cisco IP Phone, page 2-5
- Installing the Cisco IP Phone Models 7905G and 7912G, page 2-6
- Verifying Installation, page 2-15

Providing Power to the Cisco IP Phone

The Cisco IP Phone can be powered by the following sources:

- External power—optional Cisco AC adapter and power cord for connecting to a standard wall receptacle.
- Inline power—provided to the Cisco IP Phone when connected to a Cisco Catalyst switch that is capable of providing inline power.

Note Only the network port supports inline power from the Cisco Catalyst switches. The network port is labelled "10 BASET" on the Cisco IP Phone 7905G and "10/100 SW" on the Cisco IP Phone 7912G.

- WS-PWR-PANEL—power patch panel that allows the Cisco IP Phone to be connected to existing Catalyst 4000, 5000, and 6000 family 10/100BaseTX switching modules.

  This module sends power on pins 4, 5, 7, & 8, which are not used for Ethernet signaling. The power patch panel attempts to verify that the attached device is a Cisco IP Phone before providing power.

Related Topics

- Safety, page 2-2
- Connecting to the Network, page 2-4
- Installing the Cisco IP Phone Models 7905G and 7912G, page 2-6
- Power Source Design, page 2-5
- Redundancy Feature, page 2-6
- Verifying Installation, page 2-15

Power Source Design

The phone and switch automatically determine which power source the phone uses. If the power switches to a different source, the phone user will experience different results based on which power source is being used by the phone.

Use the following information to choose a power source for the phone:

- If you plug a phone into the optional power supply before plugging it into the network, the phone is powered by the power supply.
- If you then unplug the phone from the power supply, the phone resets. If the switch port is configured for 10/100 Mbps, the switch recognizes the loss of power and brings the phone back up.
- If the switch port is configured for 10 Mbps only, then you must unplug the network connection and plug it back into the phone for the switch to recognize the phone's loss of power.
- If, however, you plugged the network connection into the phone before you plugged in the power cord, the phone receives power through the switch, and unplugging the power cord will not bring down the phone. If the switch reboots, the phone will then be powered by the power cord.

Redundancy Feature

For redundancy, you can use the Cisco AC adapter even if you are using inline power from the Cisco Catalyst switches. The Cisco IP Phone can share the power load being used from the inline power and external power source. If either the inline power or the external power goes down, the phone can switch entirely to the other power source.

To use this redundancy feature:

1. Set the inline power mode to auto on the Cisco Catalyst switch.
2. Connect the unpowered Cisco IP Phone to the network.
3. Connect the external power supply to the phone after the phone powers up.

Installing the Cisco IP Phone Models 7905G and 7912G

You must install and configure the Cisco IP Phone before it will operate. Installation consists of making power and network connections. Configuration consists of setting values for various parameters.

Most frequently, the configuration parameter-value pairs for each phone are contained in a configuration file known as a *profile* that is stored on a TFTP server on the network. When the phone powers up, it contacts the TFTP server and downloads its profile. To do so, however, the phone must first receive a basic configuration that instructs it to download its profile from the TFTP server and informs it of the server location. This basic configuration can be preprogrammed on the phone before it is shipped to the end user, or it can be performed by the end user when the phone is installed.

For more information about configuring a phone, see Chapter 3, "Configuring the Cisco IP Phone Models 7905G and 7912G for SIP." For detailed information about profiles, see Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server."

The following sections describe how to install the Cisco IP Phone models 7905G and 7912G:

- Physical Installation of the Cisco IP Phone Models 7905G and 7912G, page 2-7
- Mounting the Phone to the Wall, page 2-12
- Basic Configuration of the Cisco IP Phone Models 7905G and 7912G, page 2-13

Related Topic

- Safety, page 2-2

Physical Installation of the Cisco IP Phone Models 7905G and 7912G

To install the Cisco IP Phone models 7905G and 7912G, perform the following steps.

See Figure 2-1 as you install the Cisco IP Phone 7905G, or see Figure 2-2 as you install the Cisco IP Phone 7912G.

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.**

Caution Do not cover or block the air vents on the back side of the Cisco IP Phone. Overheating can cause permanent damage to the unit.

Caution If you plan to power your phone locally (instead of receiving power through the Ethernet connection), use only a Cisco 48 volt power supply designed to work with a Cisco IP Phone.

Note Do not use hooded cables with the Cisco IP Phone models 7905G and 7912G because they can cause the phone to rock.

Procedure

Step 1 Use a Category 3 or 5 straight-through Ethernet cable to connect the 10BASET port on the Cisco IP Phone 7905G or the 10/100 SW port on the Cisco IP Phone 7912G to an Ethernet port.

Step 2 Connect the handset to the handset port.

Ensure that the end of the cord with the longer uncoiled section is connected to the body of the phone.

Step 3 Connect a Category 3 or 5 Ethernet cable to the 10/100 PC port on the back of the Cisco IP Phone 7912G (optional).

Use a crossover Ethernet cable to connect from the access port to another Ethernet device (such as a router or desktop computer) without using a hub. Otherwise, use a straight-through Ethernet cable.

The Cisco IP Phone 7905G does not have a 10/100 PC port.

Step 4 If the phone will not receive power through the Ethernet connection, connect the power supply plug to the DC adapter port on the back of the phone. Then use the power cable to connect the power supply to a standard power outlet.

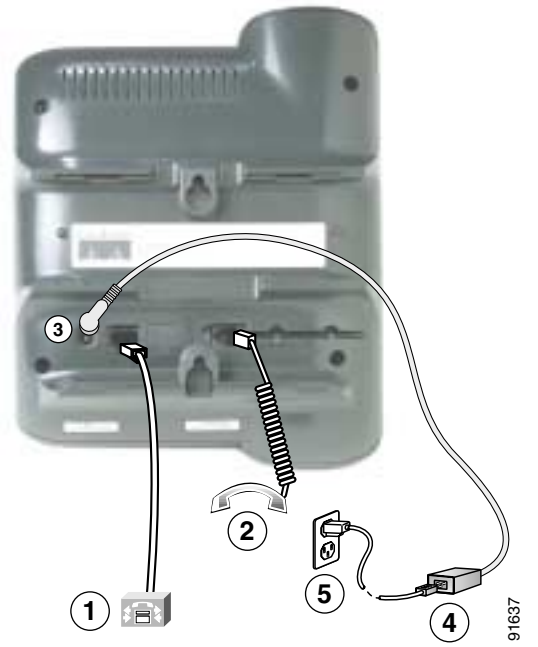
After you connect a Cisco IP Phone to its power source, a startup process begins. After several minutes, the LCD displays a neutral “ready” screen. The details on the screen might vary, but a ready screen typically displays the date and time, extension number, and available softkeys. Startup is complete and the phone is ready to use.

Softkeys point to feature options displayed along the bottom of the LCD screen. Softkeys are flexible—they change depending on the status of the phone. For example, one set of softkey options appears when the handset is picked up, and another set appears when the phone is not in use.

If the phone was preprogrammed with its basic configuration, it begins to automatically download its complete profile from the TFTP server. the initial preloaded boot load firmware image is upgraded to a firmware image that supports a specific signalling protocol.

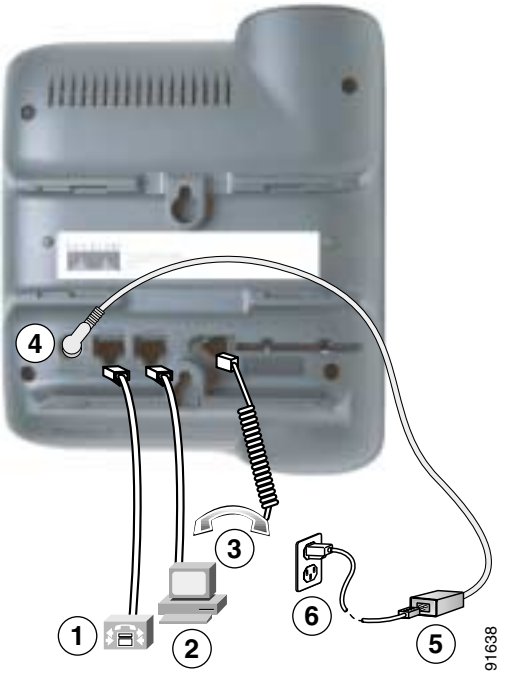
You or the end user must complete the steps in the “Basic Configuration of the Cisco IP Phone Models 7905G and 7912G” section on page 2-13 before using the phone.

Figure 2-1 Cisco IP Phone 7905G Cable Connections



1	Network port (10BASE-T)	Connects the phone to the Ethernet port in your workspace
2	Handset port	Connects the handset to the phone
3	DC adapter port (48VDC)	Connects the power supply plug to the phone
4	Power supply with DC output connector (if included)	Connects to the AC power cable
5	AC power cable with wall socket plug (if included)	Connects the power supply to a standard power outlet

Figure 2-2 Cisco IP Phone 7912G Cable Connections



1	Network port (10BASE-T, 100BASE-T)	Connects the phone to the Ethernet port in your workspace.
2	Access port (10BASE-T, 100BASE-T)	Connects the phone to the Ethernet port in a desktop computer
3	Handset port	Connects the handset to the phone
4	DC adapter port (48VDC)	Connects the power supply plug to the phone
5	Power supply with DC output connector (if included)	Connects to the AC power cable
6	AC power cable with wall socket plug (if included)	Connects the power supply to a standard power outlet

Related Topics

- Mounting the Phone to the Wall, page 2-12
- Basic Configuration of the Cisco IP Phone Models 7905G and 7912G, page 2-13

Mounting the Phone to the Wall

You can mount the Cisco IP Phone on the wall by removing the footstand and using the mounting bracket on the back of the phone, or you can use special brackets available in a Cisco IP Phone wall mount kit. (A wall mount kit must be ordered separately from the phone.) If you attach the Cisco IP Phone to the wall using the standard footstand and not the wall mount kit, you need to supply the following tools and parts:

- Screwdriver
- Screws to secure the Cisco IP phone to the wall

To mount the phone on the wall using its mounting bracket, follow these steps:

Procedure

Step 1 Remove the footstand from the phone.

Step 2 Modify the handset rest so that the handset remains on the ear-piece rest when the phone is vertically placed.

a. Remove the handset from the ear-piece rest.

b. Locate the tab (handset wall hook) at the base of the ear-piece rest.

c. Slide this tab out, rotate it 180 degrees (left to right) to expose a lip on which the handset catches when the phone is vertical, and reinsert this tab.

d. Place the handset on the ear-piece rest.

For an illustrated procedure of modifying the handset rest, refer to *Installing the Wall Mount Kit for the Cisco IP Phone*.

Step 3 Insert two screws into a wall stud or into wall anchors, matching the screws to the two screw holes on the back of the phone.

The keyholes fit standard phone jack mounts.

Step 4 Hang the phone on the wall.

Basic Configuration of the Cisco IP Phone Models 7905G and 7912G

The basic configuration of a Cisco IP Phone provides the phone with the minimal information that it needs to download its complete operational configuration profile from a TFTP server. This information includes a value to enable TFTP downloads, a value for the URL for the TFTP server that stores the phone's complete configuration file (also known as a *profile*), and a value for the encryption key.

The following steps explain how to perform this basic configuration for the Cisco IP Phone.As administrator, you can preconfigure a phone before it is shipped to the end user. Then, after the end user connects a phone as described in the "Physical Installation of the Cisco IP Phone Models 7905G and 7912G" section on page 2-7, the phone automatically downloads the configuration profile and the latest phone software from the TFTP server. The phone is ready for use within seconds.

If preconfiguration is not possible, the end user can perform these steps after connecting the phone.

Procedure

Step 1 Press the **Menu** button to access the Services menu.

Step 2 In the Services menu, use the **Navigation** button to select **Settings**, and then press the **Select** softkey.

Step 3 In the Settings menu, use the **Navigation** button to select **Network Configuration**, and then press the **Select** softkey.

Step 4 Unlock network configuration settings.

For instructions, see the "Unlocking and Locking Configuration Parameters" section on page 5-4.

Step 5 In the Network Configuration menu, use the **Navigation** button to select **Alternate TFTP**, and then press the **Yes** softkey.

Step 6 In the Network Configuration menu, use the **Navigation** button to select **TFTP Server**, and then press the **Edit** softkey.

The current value for the IP address of the TFTP server appears in the Current Value and the New Value fields.

Step 7 Enter a new IP address in the New Value field.

Use the arrow softkey (<<) to delete existing characters. Use the ***** key on the keypad to enter a period (.).

Note When the cursor moves over a character, the character is deleted and a new character must be entered. You cannot cancel individual character deletions, but you can use the **Cancel** softkey to back out of the screen without saving your changes.

Step 8 Press the **Validate** softkey.

Step 9 In the Network Configuration menu, use the **Navigation** button to select **Profile Encrypt Key**, and then press the **Edit** softkey.

Step 10 Enter the encryption key using the keys on the keypad, and then press the **Validate** softkey.

For information about entering alpha-numeric characters, see the "Editing Parameter Values" section on page 5-5.

Step 11 Press the **Save** softkey.

Step 12 Press the **Back** softkey and then press the **Exit** softkey.

The phone downloads its configuration profile and the latest phone software from the TFTP server.

Verifying Installation

If you hear a dial tone when you lift the handset, you have installed the Cisco IP Phone properly. If you experience any problems, see Chapter 9, "Troubleshooting the Cisco IP Phone Models 7905G and 7912G."

Configuring the Cisco IP Phone Models 7905G and 7912G for SIP

This chapter provides an overview of configuring the Cisco IP Phone to operate with the SIP firmware image.

This chapter includes the following sections:

- Overview of Configuration Methods, page 3-1
- Default Boot Load Behavior, page 3-2
- Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation, page 3-4
- Basic Configuration Steps in a TFTP Server Environment, page 3-6
- Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G, page 3-9

Overview of Configuration Methods

You can configure the Cisco IP Phone for SIP by using any of these methods:

- TFTP server—Recommended method for deploying a large number of Cisco IP Phones. This method allows you to set up a unique configuration file for each phone or to set up a configuration file that is common to all Cisco IP phones. These configuration files are called *profiles*. The

Cisco IP Phone can automatically download its latest profile from the TFTP server when the phone powers up, is refreshed or reset, or when the specified TFTP query interval expires.

For more information, see Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server."

- Phone configuration menus—Manual method for configuring an individual phone. Each Cisco IP Phone includes menus for configuring a variety of network and SIP settings.

  For more information, see Chapter 5, "Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus."

- Phone web page—Convenient if you plan to deploy a small number of Cisco IP Phones in your network. To use this method, the phone must first obtain IP connectivity

  For more information, see Chapter 7, "Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages."

Related Topics

- Default Boot Load Behavior, page 3-2
- Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation, page 3-4
- Basic Configuration Steps in a TFTP Server Environment, page 3-6
- Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G, page 3-9

Default Boot Load Behavior

Before you configure the Cisco IP Phone, you need to know how the default boot load process works. Once you understand this process, you will be able to configure the phone by following the instructions provided in this section and in the sections that follow.

It is important to understand the boot load process because if your network environment is not set up to follow this default behavior, you will need to make the applicable configuration changes. For example, by default, the Cisco IP Phone attempts to contact a DHCP server for the necessary IP addresses to achieve

network connectivity. However, if your network does not use a DHCP server, you must manually configure the IP address of the phone, the subnet mask used by the phone, and the network gateway (default router) IP address for the phone.

All Cisco IP Phones are shipped with a bootload image. However, because this image is not a fully-functional signaling image, the image must be upgraded. The image is designed to be automatically upgraded by a properly configured TFTP server. To configure the Cisco IP Phone to automatically upgrade to the latest signaling image, see the "Upgradecode Parameter Detail" section on page 8-41.

In addition, the Cisco IP Phone obtains its configuration file during the bootload process.

Here is a summary of the default Cisco IP Phone behavior during its boot-up process:

1. The Cisco IP Phone uses the Cisco Discovery Protocol (CDP) to discover which VLAN to enter. If the phone receives a VLAN ID response from the network switch, the phone enters that VLAN and adds 802.1Q VLAN tags to its IP packets. If the phone does not receive a response with a VLAN ID from the network switch, the phone assumes it is not operating in a VLAN environment and does not perform VLAN tagging on its packets.

Note If your network environment is not set up to handle this default behavior, make the necessary configuration changes by referring to the "Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation" section on page 3-4.

2. The phone contacts the DHCP server to request its own IP address.

Note If your network does not use a DHCP server, you must manually configure the IP address of the phone, the subnet mask used by the phone, and the network gateway (default router) IP address for the phone. For more information, see the "Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G" section on page 3-9.

3. The phone also requests the IP address of the TFTP server from the DHCP server.

4. The phone downloads a profile from the TFTP server. To do so, it requests the following profiles from the TFTP server, in the order shown, until a file exists. Then it downloads that file. In the file names, *xxxxxxxxxxxx* is the hexadecimal representation of the phone's MAC address. (The first three files are not used for SIP. They are included for compatibility reasons.)
   - SEP*xxxxxxxxxxxx*.cfg.xml
   - XMLDefault.cnf.xml
   - SEPDefault.cnf
   - ld*xxxxxxxxxxxx* (for the Cisco IP Phone 7905G) or gk*xxxxxxxxxxxx* (for the Cisco IP Phone 7912G)
   - lddefault.cfg (for the Cisco IP Phone 7905G) or gkdefault.cfg (for the Cisco IP Phone 7912G)

Related Topics

- Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation, page 3-4
- Basic Configuration Steps in a TFTP Server Environment, page 3-6
- Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G, page 3-9

Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation

If you want the Cisco IP Phone to use a preconfigured VLAN ID instead of using the Cisco Discovery Protocol to locate a VLAN, or if you want to disable VLAN IP encapsulation, you may need to configure the following parameters. (For more information about these parameters, see the "Network Parameters" section on page 8-2.) See Table 3-1 for information about which VLAN-related parameters and bits to configure depending on your network environment.

- OpFlags parameter:
  - Bit 4—Enable the use of user-specified voice VLAN ID
  - Bit 5—Disable VLAN IP encapsulation
  - Bit 6—Disable CDP discovery

- VLANSetting parameter:
  - Bits 0-2—Specify VLAN CoS bit value (802.1Q priority) for signaling packets
  - Bits 3-5—Specify VLAN CoS bit value (802.1Q priority) for audio packets
  - Bits 18-29—User-specified 802.1Q VLAN ID

Table 3-1 VLAN-Related Features and Corresponding Configuration Parameters

Feature	OpFlags Bit 4	OpFlags Bit 5	OpFlags Bit 6	VLANSetting Bits 18-29
Static VLAN	1	0	1	VLAN ID
CDP-acquired VLAN	0	0	0	Not applicable[1]
No VLAN	—	1	—	Not applicable[1]
No CDP	—	—	1	Not applicable[1]
No CDP and no VLAN	0	1	1	Not applicable[1]

1. This variable is not applicable to the feature and the setting of this variable does not affect the feature.

Example

The following procedure shows you how to configure the OpFlags and VLANSetting parameters to allow the phone to use a user-specified VLAN ID. In this example, the voice VLAN ID is 115 (in decimal format).

Step 1 Set bits 4-6 of the OpFlags parameter to 1, 0, and 1, respectively. This setting translates to the following bitmap:

```
xxxx xxxx xxxx xxxx xxxx xxxx x101 xxxx
```

The remaining bits of the OpFlags parameter, using all default values, make up the following bitmap representation:

```
0000 0000 0000 0000 0000 0000 0xxx 0010
```

Therefore, the resulting value of the OpFlags parameter becomes the following bitmap representation:

```
0000 0000 0000 0000 0000 0000 0101 0010
```

In hexadecimal format, this value is 0x00000052.

Step 2 Set bits 18-29 of the VLANSetting parameter to voice VLAN ID 115. This setting translates to the following bitmap

```
xx00 0001 1100 11xx xxxx xxxx xxxx xxxx
```

where 000001110011 is the binary representation of the decimal value 115.

The remaining bits of the VLANSetting parameter, using all default values, make up the following representation:

```
00xx xxxx xxxx xx00 0000 0000 0010 1011
```

Therefore, the resulting value of the VLANSetting parameter becomes the following bitmap representation:

```
0000 0001 1100 1100 0000 0000 0010 1011
```

In hexadecimal format, this value is 0x01cc002b.

Related Topics

- Default Boot Load Behavior, page 3-2
- Basic Configuration Steps in a TFTP Server Environment, page 3-6
- Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G, page 3-9

Basic Configuration Steps in a TFTP Server Environment

The following table shows the basic steps for upgrading the firmware image for a Cisco IP Phone, configuring the phone, and making it operational in a typical SIP environment, which includes a TFTP server.

	Procedure	Reference
Step 1	Download the desired phone release software zip file from the Cisco website and store it on the TFTP server.	See the "Setting Up the TFTP Server with Cisco IP Phone Software" section on page 6-4.
Step 2	Follow these basic steps to create a unique profile, which actually entails creating two files: 1. Create a phone profile that contains parameters that are common to all Cisco IP Phones in your network. 2. Create a unique profile text file that contains parameters that are specific to a Cisco IP Phone. Make sure to use an **Include** parameter in the unique profile to pull in values from the common configuration file. 3. Convert the unique configuration file to binary format. 4. Place the unique binary configuration file on the TFTP server.	See Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server."
Step 3	Optionally, create a default profile called lddefault.cfg for the Cisco IP Phone 7905G or gkdefault.cfg for the Cisco IP Phone 7912G, which the phone will download from the TFTP server only if the unique profile called ld*xxxxxxxxxxxx* or gk*xxxxxxxxxxxx* does not exist on the TFTP server.	See the "Creating a Default Profile" section on page 6-13.
Step 4	Configure the upgradecode parameter so that the phone will obtain the correct signaling image from the TFTP server when the phone powers up.	See the "Upgradecode Parameter Detail" section on page 8-41.

	Procedure	Reference
Step 5	Configure the desired interval for the phone to contact the TFTP server to check for a configuration-file update or an upgrade of the signaling image file. Use the CfgInterval parameter to set this interval.	See the "Network Parameters" section on page 8-2.
Step 6	Configure the method by which the phone will locate the TFTP server at boot up time.	See the"Configuring the Cisco IP Phone to Obtain its Configuration File from the TFTP Server" section on page 6-5.
Step 7	Power up the phone.	—
Step 8	If you make configuration changes to the phone or if you upgrade the signaling image on the TFTP server, you can refresh the phone so that these changes take effect immediately. Otherwise, these changes will take effect when the specified interval (CfgInterval parameter value) for the TFTP query expires.	See the "Refreshing or Resetting the Cisco IP Phone" section on page 6-17.

Table 4-1 on page 4-2 contains a list of all required SIP parameters. These parameters must be properly configured for the Cisco IP Phone to work.

For descriptions of important Cisco IP Phone SIP services that you can configure, and references to their configuration parameters, see the "Important Basic SIP Services" section on page 4-2 and the "Additional SIP Services" section on page 4-4.

Table 4-3 on page 4-12 lists, in alphabetical order, various features that you can configure for the Cisco IP Phone.

Related Topics

- Default Boot Load Behavior, page 3-2
- Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation, page 3-4
- Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G, page 3-9

Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G

The Cisco IP Phone requires the following minimum settings for network connectivity:

- IP address
- Subnet mask
- Network gateway (default router) IP address

These settings can be configured using any of the methods described in the following sections:

- Making Settings with a DHCP Server, page 3-9
- Making Settings Manually, page 3-10

Related Topics

- Default Boot Load Behavior, page 3-2
- Specifying a Preconfigured VLAN ID or Disabling VLAN IP Encapsulation, page 3-4
- Basic Configuration Steps in a TFTP Server Environment, page 3-6

Making Settings with a DHCP Server

If your Cisco IP Phone network contains a DHCP server, the Cisco IP Phone automatically learns its IP address, subnet mask, and network gateway from the DHCP server when the phone starts up.

Making Settings Manually

If your network does not use a DHCP server, you must manually specify the IP address of the phone, the subnet mask used by the phone, and the network gateway (default router) IP address for the phone. You can specify this information using the phone's Network Configuration menu, using a profile, or using a phone's web page.

When you manually specify these values, you must disable DHCP by using the DHCP Enabled parameter on the Network Configuration menu or the Dhcp parameter in a profile or web page.

To manually specify the IP address, subnet mask, and default router IP address, use these parameters:

Setting	Parameter on Network Configuration Menu	Parameter in Profile or on Web Page
IP address of a phone	IP Address	StaticIP
Subnet mask used by the phone	Subnet Mask	StaticNetMask
Network gateway (default router) IP address used by the phone	Default Router	StaticRoute

For detailed information about configuring menus on the phone, see Chapter 5, "Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus."

For detailed information about configuring through profiles, see Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server."

For detailed information about configuring through a phone's web page, see Chapter 7, "Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages."

Basic and Additional SIP Services

This chapter provides information about configuring SIP services that are supported on the Cisco IP Phone models 7905G and 7912G. For detailed information about any parameter mentioned in the following sections, see Chapter 8, "Profile and Web Page Parameters and Defaults."

This chapter includes these topics:

- Important Basic SIP Services, page 4-2—Describes parameters that you must configure for the Cisco IP Phone to function in a SIP environment.
- Additional SIP Services, page 4-4—Contains information about additional, commonly used SIP features, with references to the parameters for configuring these services.
- Complete Reference of all Cisco IP Phone SIP Services, page 4-12—Contains a complete listing of Cisco IP Phone services that are supported for SIP, and includes cross references to the parameters for configuring these services. Includes services not described in the sections about the basic SIP services and the commonly used additional SIP services.

Important Basic SIP Services

This section provides descriptions and cross references for configuring required SIP parameters and for configuring other important basic SIP services. This section includes these topics:

- Required Parameters, page 4-2
- Establishing Authentication, page 4-4
- Configuring Refresh Interval, page 4-4

Required Parameters

Table 4-1 shows the SIP parameters that you must supply for a Cisco IP Phone. The Parameter fields in this table show each parameter name as it appears on a phone's web page or in its profile ("web page or profile"), or on the phone's Network Configuration menu or SIP Configuration menu ("on phone menu").

For more detailed explanations of these parameters, see Chapter 5, "Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus," and Chapter 8, "Profile and Web Page Parameters and Defaults." These chapters also contain information about other configuration parameters.

Table 4-1 Required SIP Parameters and Defaults

Parameter	Description	Minimum Value	Maximum Value	Default Value
SIPRegInterval (web page or profile) Register Expires (on phone menu)	Number of seconds between registration renewal.	1	86400	3600
MAXRedirect (web page or profile)	Maximum number of times to try redirection.	0	10	5
SIPRegOn (web page or profile) Register with Proxy (on phone menu)	Enable SIP registration.	0	1	0

Table 4-1 Required SIP Parameters and Defaults (continued)

Parameter	Description	Minimum Value	Maximum Value	Default Value
NATIP (web page or profile) NAT WAN IP Address (on phone menu)	WAN address of the attached router/NAT; currently only used to support SIP behind a NAT.	—	—	0.0.0.0
SIPPort (web page or profile) Local SIP Port (on phone menu)	Port to listen for incoming SIP requests.	1	65535	5060
MediaPort (web page or profile) Local RTP Port (on phone menu)	Base port to receive RTP media.	1	65535	16384
OutBoundProxy (web page or profile) Outbound Proxy (on phone menu)	Outbound proxy server IP address or fully qualified domain name (FQDN) for all outbound SIP requests. All SIP requests are sent to OutBoundProxy, when configured, instead of to the configured Proxy.	—	—	0
Proxy (web page or profile) SIP Proxy (on phone menu)	SIP proxy server IP address or fully qualified domain name (FQDN).	—	—	0

Establishing Authentication

The UseLoginID parameter lets you select the user ID for authentication of the phone to the remote end as follows:

- If UseLoginID is set to 0, the user ID (set with the UID parameter) is used with a user-supplied password (set with the PWD parameter) for authentication.
- If UseLoginID is set to 1, you must supply a login ID (set with the LoginID parameter) and a password (set with the PWD parameter) for authentication.

Configuring Refresh Interval

When the value specified with the CfgInterval parameter is reached, the Cisco IP Phone attempts to refresh its configuration file from the TFTP server. (You can manually perform a refresh before the scheduled refresh as explained in the "Refreshing the Cisco IP Phone" section on page 6-17.)

When a Cisco IP Phone contacts the TFTP server, it also checks to see if a firmware image has been placed on the TFTP server. If such an image exists, the phone will download this image.

Additional SIP Services

Table 4-2 describes additional SIP services and provides references to additional information. These services are listed alphabetically.

Note Many of the descriptions in Table 4-2 refer to specific parameters that you can set in a profile or from a phone's web page. For the corresponding parameter in the phone configuration menus, see Appendix B, "Phone Menu, Web Page, and Profile Equivalent Parameters."

Table 4-2 Additional SIP Services

SIP Service	Description	Reference
Advanced audio configuration.	The TOS parameter (which specifies the default IP precedence of UDP packets) and AudioMode parameter (which specifies the audio operating mode) allow you to tune audio configuration.	See the "SIP Parameters" section on page 8-9 and the "Audio Parameters" section on page 8-24.
Call preferences	The GUI Show Mask or CallPrefGuiShow specify which parameters, if any, appear on the Call Preferences menu on the phone. The GUI Set Mask or CallPrefGuiSet parameters specify which parameters on the Call Preferences menu on the phone can be changed by an end user. You can use these parameters to offer specific features on a subscription basis	See the "Call Preference Parameters" section on page 8-13.
Comfort noise	When silence suppression is turned on in G.711, the Cisco IP Phone calculates and transmits its noise level to the far end to enable the remote endpoint to generate the appropriate amount of comfort noise. This feature provides the remote user with a similar experience to that of a PSTN call and prevents silent gaps when neither party is talking. You enable or disable silence suppression with bit 0 in the AudioMode parameter.	See the "Audio Parameters" section on page 8-24.
Debugging diagnostics	You can use the following parameters to troubleshoot operation issues: • NPrintf—Specifies the IP address and port where debug information is sent. • TraceFlags—Turns on specific trace features.	See the "Network Parameters" section on page 8-2.
Dial plan	You can use the DialPlan parameter to set specific dial plan rules and timeout values. Many of these values are determined on a country-by-country basis.	See the "SIP Parameters" section on page 8-9.
Disabling access to the web interface	To prevent tampering and unauthorized access to the Cisco IP Phone configuration, you can use the OpFlags parameter to prevent configuring the phone through the web.	See the "Network Parameters" section on page 8-2.

Table 4-2 Additional SIP Services (continued)

SIP Service	Description	Reference
Distinctive ringing support	If an incoming INVITE contains an Alert-Info header with the name Bellcore-dr1, Bellcore-dr2, Bellcore-dr3, Bellcore-dr4, or Bellcore-dr5, the phone will play the ring pattern r_n, where n = 1, 2, 3, 4, or 5 as specified in Bellcore GR506. If the Alert-Info header is not present or if the ring pattern name is unknown, the phone will play the default ring pattern Bellcore-dr1.	—
DNS SRV support	The Cisco IP Phone supports DNS SRV lookup for the SIP proxy server. If the Proxy parameter value is a domain name, the phone performs a DNS SRV lookup for the SIP proxy server. A DNS SRV lookup results in one of the following conditions: • Zero host is returned or DNS SRV lookup failed. The phone then performs a regular DNS A-record lookup for the given name. • One host is returned. The single host is used as the primary proxy farm. • Two or more hosts are returned. The two hosts with the highest priorities are used as the primary and backup proxy farms.	See the "SIP Parameters" section on page 8-9.
Hardware information	You can view Cisco IP Phone hardware information on the phone's Model Information menu and on the Device Information area in a phone's web page.	See the "Model Information Menu" section on page 5-17 and the "Device Information" section on page 7-4.

Table 4-2 Additional SIP Services (continued)

SIP Service	Description	Reference
NAT gateway	Network Address Translation (NAT) supports port mapping and forwarding to standard default SIP signaling port 5060 and media base port 16384, or other ports as configured for the Cisco IP Phone. Media ports are evenly numbered from the base port. NAT must support multiple port mappings. The phone can use up to four media ports to handle conference calls on both lines. For example, if media base port 16384 is used for one call, the next call uses port 16386 and other calls will use ports 16388 and 16390. (Routers such as D-Link, WinRoute, and WinProxy may not route correctly if both caller and callee are behind the same NAT.) To configure the phone to work in a NAT environment, make the following settings: • Use the StaticRoute parameter to specify the LAN IP address of the NAT through which the phone will communicate. • Use the NATIP parameter to specify the WAN IP address of the NAT through which all external SIP user agents will communicate. • Optionally use the SIPPort parameter to specify a new port for SIP messages. • Optionally use the MediaPort parameter to specify a new base port for RTP media.	See the "Network Parameters" section on page 8-2 and the "SIP Parameters" section on page 8-9.

Table 4-2 Additional SIP Services (continued)

SIP Service	Description	Reference
NAT/PAT translation	To maintain Network Address Translation/Port Address Translation (NAT/PAT) for a session, the Cisco IP Phone can be configured to periodically send a dummy UDP packet to a server (the phone does not expect any response from the server). To specify this configuration, use these parameters: • NatTimer—Bits 0 to 11 are for specifying the retransmission period. • NatServer—Specifies the server to which the dummy packet is sent.	See the "SIP Parameters" section on page 8-9.
Network timing	You can fine tune your network timing by making the following settings: • Use the TimeZone parameter to specify the time-stamp for incoming calls (offset from Greenwich Mean Time). • Use the NTPIP parameter to specify the IP address of the Network Time Protocol (NTP) server. NTP is a protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. • Use the AltNTPIP parameter to specify an alternate NTP server IP address. • Use the ConnectMode parameter to specify the connection mode of the SIP protocol.	See the "Network Parameters" section on page 8-2 and the "Audio Parameters" section on page 8-24.

Table 4-2 Additional SIP Services (continued)

SIP Service	Description	Reference
Proxy Redundancy support	The Cisco IP phone supports next hop server redundancy when a fully qualified domain name (FQDN) is specified for the Proxy or Outbound Proxy parameter. When sending a SIP request, the phone performs a DNS SRV records query for the domain name. The phone selects two records from the result and identifies them as Primary Proxy Farm (PPF) and Alternate Proxy Farm (APF). Each farm may contain up to five IP addresses. If a DNS SRV record does not exist, the phone performs a DNS A records query for the domain name, which is now considered the Primary Proxy Farm with no Alternate Proxy Farm. The phone accepts up to five IP addresses from the query result. The phone retries with the alternate next hop server for the following SIP requests: REGISTER, INVITE, CANCEL, BYE, REFER, and NOTIFY. If sending one of these requests results in a 5xx response, no response, or ARP timeout, the phone attempts the same request with an alternate destination IP address derived from the next hop domain name. If both primary and alternate farms exist, the phone attempts the primary farm first and then the alternate farm. The phone will attempt all the IP addresses in one farm before switching to the other farm. Once the phone finds a responding next hop server, it remembers the farm and IP address of the server and keeps using it for the given domain name until it fails or expires. If the request still fails after all the possible IP addresses are attempted, the phone considers the request as failed. If a server in the alternate proxy farm is active at the moment, the phone can be configured to retry the primary proxy farm after the number of seconds specified by the AltProxyTimeout parameter. If this value is 0, the phone remains with the alternate proxy farm until all the IP addresses in the farm are down before attempting the primary proxy farm again.	See the "SIP Parameters" section on page 8-9.

Table 4-2 Additional SIP Services (continued)

SIP Service	Description	Reference
Progress tones	Values for the following parameters must be determined based on the country in which the Cisco IP Phone is located: • DialTone • DialTone2 • BusyTone • ReorderTone • RingBackTone • CallWaitTone	See the "Tone Parameters" section on page 8-21.
Receiver-tagged VIA header	You can use the ConnectMode parameter to disable or enable the processing of the *received* = parameter in the Via header. This feature is disabled by default.	See the "Audio Parameters" section on page 8-24.
Setting up and placing a call without using a SIP proxy	You can user the Cisco IP Phone to make a direct IP-to-IP calls without using a SIP proxy.	See the "Setting Up and Placing a Call Without Using a SIP Proxy" section on page 4-10.

Setting Up and Placing a Call Without Using a SIP Proxy

The Cisco IP Phone models 7905G and 7912G support direct IP-to-IP calls without using a SIP proxy. When a call is placed, the phone sends the INVITE request directly to the remote user agent and expects the usual 100/180/200 responses from the user agent.

To configure a Cisco IP Phone for calls that do not use a SIP proxy, set the following parameters to the values shown:

Parameter on SIP Configuration Menu	Parameter in Profile or on Web Page	Setting
SIP Proxy	Proxy	0 (zero) or No
User ID	UID	Telephone number of the phone
Register with Proxy	SipRegOn	0 (zero) or No (disables SIP registration with a SIP proxy server)

To place an IP call, dial the telephone number and the IP address of the remote user agent using this format:

*phone_number***IPaddress*

Use the star (*) key on the telephone keypad to represent the dot (.) in an IP address. If you are using on-hook dialing, press the **Dial** softkey to terminate the dial string and place the call. If you are using off-hook dialing, press the pound (#) key on the telephone keypad to terminate the dial string and place the call

Note URL dialing is not supported.

For example, to place a call to a user agent with an ID of 408-555-1212 at IP address 192.168.1.100, enter the following string on your telephone keypad:

4085551212192*168*1*100**

Related Topics

- Chapter 5, “Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus,”
- Chapter 6, “Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server,”
- Chapter 7, “Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages.”
- Chapter 8, “Profile and Web Page Parameters and Defaults.”

Complete Reference of all Cisco IP Phone SIP Services

Table 4-3 lists all configurable features for the Cisco IP Phone using SIP. It also lists the names of the parameters used to configure the features.

Table 4-3 Configurable Features and Related Parameters

Configurable Feature	Related Parameter in Profile or on Web Page	Related Parameter on Phone Menu
802.1Q packet tagging	VLANSetting	Admin. VLAN Id
Backup proxy timeout	AltProxyTimeOut	Backup Proxy Timeout
Call forward	CallForwardNumber (in profile) Call Forward Number (on web page)	Call Forward Number
Call forwarding—Maximum times allowed	MAXRedirect	—
Call Preferences	GUI Show Mask and GUI Set Mask (on web page) CallPrefGuiShow and CallPrefGuiSet (in profile)	Parameters on Call Preference menu
Call waiting tone period	SigTimer	—
Cisco Discovery Protocol	OpFlags	—
Configuration update interval	CfgInterval	—
Debug messages—configuring host	NPrintf	—
DialPlan	DialPlan	—
Primary domain name server (DNS)	DNS1IP	DNS Server 1
DTMF signaling method	AudioMode	—
Encryption	EncryptKey	Profile Encrypt Key
IDs for phone lines	UID	User ID

Table 4-3 Configurable Features and Related Parameters (continued)

Configurable Feature	Related Parameter in Profile or on Web Page	Related Parameter on Phone Menu
IP-like address in dial plan	IPDialPlan	—
Login ID	LoginID	Login ID
NTP IP address	NATIP	NAT WAN IP Address
Outbound proxy	OutBoundProxy	Outbound Proxy
Password for registration and authentication	PWD	Password
Primary NTP server	NTPIP	NTP Server 1
Received= tag processing enable/disable	ConnectMode	—
Receiving-audio codec preference	RxCodec	—
Refresh phone using web server	OpFlags	—
REGISTER action types	ConnectMode	—
Registration removal	ConnectMode	—
Reset phone using web server	OpFlags	—
Retransmission interval for NAT server	NatTimer	—
Ringback tone—send to caller	ConnectMode	—
Ring-cadence pattern	RingOnOffTime	—
RTP media port	MediaPort	Local RTP Port
RTP packet size	NumTxFrames	—
RTP statistics	TraceFlags	—
Secondary domain name server	DNS2IP	DNS Server 2
Secondary NTP server	AltNTPIP	NTP Server 2
Server to which to send dummy packets to maintain port mappings	NatServer	—
Silence compression	AudioMode	—
SIP proxy address	Proxy	SIP Proxy
SIP registration renewal interval	SIPRegInterval	Register Expires
SIP registration enable/disable	SIPRegOn	Register with Proxy

Table 4-3 Configurable Features and Related Parameters (continued)

Configurable Feature	Related Parameter in Profile or on Web Page	Related Parameter on Phone Menu
SIP request sending and receiving port	SIPPort	Local SIP Port
Static network router probing	OpFlags	—
TFTP file—not using internally generated name	OpFlags	—
Timeout values	SigTimer	—
Time zone offset	TimeZone	Time Zone
Tones: BusyTone, CallWaitTone, DialTone, DialTone2, ReorderTone, and RingBackTone parameters	Tone Parameters	—
Tracing	TraceFlags	—
Transmitting-audio codec preference	TxCodec	—
UDP packet default IP precedence	TOS	—
VLAN encapsulation	OpFlags	—
VLAN mode	OpFlags	—
WAN address of NAT	NATIP	NAT WAN IP Address
Web configuration—disallowing	OpFlags	—

Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus

The Cisco IP Phone includes configurable network and SIP parameters, which you might need to modify before the phone is accessible and functional for your users.

You can configure and view many parameters through configuration and status menus on the phone, as described in this chapter. You can also view and configure most parameters through web pages and all parameters through profiles. For more information, see Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server," and Chapter 7, "Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages."

Appendix B, "Phone Menu, Web Page, and Profile Equivalent Parameters," shows the configurable parameters on the phone menus and their equivalent web page and profile parameters.

Note If you configure a phone using a TFTP server, parameter values in a profile will overwrite values that you set from the phone menus for the same parameters.

This chapter includes the following sections:

- Configuration Menus on the Cisco IP Phone, page 5-2
- Network Configuration Menu, page 5-6
- SIP Configuration Menu, page 5-14

- Model Information Menu, page 5-17
- Status Menu, page 5-18

Configuration Menus on the Cisco IP Phone

The Cisco IP Phone models 7905G and 7912G include the following configuration, information, and status menus. You access each of these menus from the Settings menu on the phone.

- Network Configuration menu—Lets you view and configure a variety of network parameters. For more information, see the "Network Configuration Menu" section on page 5-6.
- SIP Configuration menu—Lets you configure variety of SIP signaling parameters. For more information, see the "SIP Configuration Menu" section on page 5-14.
- Model Information menu—Displays hardware and software information about phone. For more information, see the "Model Information Menu" section on page 5-17.
- Status menu—Provides options for displaying status messages, network statistics, and firmware versions. For more information, see the "Status Menu" section on page 5-18.
- Call Preferences menu—Controls various user features on the phone. For more information, see the "Call Preferences Menu" section on page A-1.

Before you can change parameter values on the Network Configuration menu and the SIP Configuration menu, you must unlock the parameters that appear on these menus. See the "Unlocking and Locking Configuration Parameters" section on page 5-4 for instructions.

For information about the keys you can use to edit or change parameters, see the "Editing Parameter Values" section on page 5-5.

You can also change many of the network configuration and SIP configuration parameters from the phone's profile or web page. For more information, see Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server," and Chapter 7, "Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages."

This section includes the following topics:

- Displaying a Configuration Menu, page 5-3
- Unlocking and Locking Configuration Parameters, page 5-4
- Editing Parameter Values, page 5-5

Displaying a Configuration Menu

To display a configuration menu, follow these steps:

Procedure

Step 1 Press the **Menu** button to access the Services menu.

Step 2 In the Services menu, use the **Navigation** button to select **Settings**, and then press the **Select** softkey.

Tip You can access a menu option directly by pressing on the keypad the number that appears next to the option.

Step 3 In the Settings menu, use the **Navigation** button to select the desired menu, and then press the **Select** softkey.

To exit a configuration menu and return to the main LCD screen, press the **Back** softkey until the **Exit** softkey appears, and then press the **Exit** softkey.

Related Topics

- Unlocking and Locking Configuration Parameters, page 5-4
- Editing Parameter Values, page 5-5

Unlocking and Locking Configuration Parameters

Configuration parameters in the Network Configuration menu and the SIP Configuration menu on a phone are locked by default to prevent users from making changes that could affect the operation of a phone.

When parameters are inaccessible for modification, a *locked* padlock icon appears on the Network Configuration menu and the SIP Configuration menu. When parameters are unlocked and accessible for modification, an *unlocked* padlock icon appears on these menus, as shown below.

You must unlock the network configuration parameters or the SIP configuration parameters before you can configure them. If a password has been specified for the phone, you must enter the password when unlocking configuration parameters. (For more information about passwords, see the explanation of UIPassword in Table 8-6 on page 8-26.)

Network configuration parameters and SIP configuration parameters are locked again automatically when you exit the Settings menu.

To unlock network configuration and SIP configuration parameters on the Cisco IP Phone, follow these steps:

Procedure

Step 1 Press the **Menu** button.

Step 2 Use the **Navigation** button to select **Settings**, and then press the **Select** softkey.

Step 3 Use the **Navigation** button to select **Network Configuration** or **SIP Configuration**, and then press the **Select** softkey.

Step 4 From the Network Configuration menu or the SIP Configuration menu, press ****#**.

Step 5 If your phone displays "Enter Admin Password," enter your password and then press the **Enter** softkey.

See the "Editing Parameter Values" section on page 5-5 for information about entering numbers or letters.

When parameters are unlocked, the icon in the upper-right portion of your LCD appears as an unlocked padlock.

Related Topic

- Editing Parameter Values, page 5-5

Editing Parameter Values

When you edit the value of a configuration parameter, follow these guidelines:

- Use the keys on the dial pad to enter characters (such as numbers, letters, and periods).
- If a parameter value can accept either numbers or letters, the **Number** / **Alpha** toggle softkey will be available. Press the **Number** softkey to enter numbers using the dial pad. Press the **Alpha** softkey to enter letters using the dial pad.
- To enter letters using the dial pad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the 2 key once for "a," twice quickly for "b," and three times quickly for "c." After you pause, the cursor automatically advances so you can enter the next letter.
- To enter a period (for example, in an IP address), press the ***** key on the dial pad.
- Press the << softkey if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press the **Cancel** softkey before pressing the **Validate** softkey or the **Save** softkey to discard any changes you have made.

Note After you change and save some parameter values, the phone may reset automatically.

Related Topic

- Unlocking and Locking Configuration Parameters, page 5-4

Network Configuration Menu

The Network Configuration menu lets you configure a variety of network parameters. Table 5-1 describes these parameters and explains how to change them.

Note The **Edit**, **Yes**, or **No** softkeys for changing network configuration parameters appear only if parameters are unlocked as described in the "Unlocking and Locking Configuration Parameters" section on page 5-4. For information about the keys you can use to edit parameters, see the "Editing Parameter Values" section on page 5-5.

Table 5-1 Network Configuration Menu Parameters

Parameter	Description	To Change
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains information such as its IP address, its subnet mask, and the IP addresses of the network gateway and the DNS, NTP, and TFTP servers.	Display only—cannot configure.
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only—cannot configure.
Host Name	Unique host name of the phone.	Display only—cannot configure.

Table 5-1 Network Configuration Menu Parameters (continued)

Parameter	Description	To Change
Domain Name	Network domain in which the phone resides. You can change this value if the Alternate Domain parameter is set to Yes.	1. Unlock configuration parameters. 2. Set the Alternate Domain parameter to Yes. 3. Scroll to the Domain Name parameter, press the **Edit** softkey, and then enter a new domain name. 4. Press the **Validate** softkey, and then press the **Save** softkey.
IP Address	Internet Protocol (IP) address of the phone. You can use this parameter to assign the IP address if DHCP does not provide it. If you assign an IP address with this parameter, you must also assign a subnet mask and network gateway (default router). See the Subnet Mask and the Default Router parameters in this table.	1. Unlock configuration parameters. 2. Set the DHCP Enabled parameter to No. 3. Scroll to the IP Address parameter, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey, and then press the **Save** softkey.
Subnet Mask	Subnet mask used by the phone. You can use this parameter to assign a subnet mask if DHCP does not provide it. If you assign a Subnet Mask with this parameter, you must also assign an IP address and a network gateway (default router) for the phone. See the IP Address and the Default Router parameters in this table.	1. Unlock configuration parameters. 2. Set the DHCP Enabled parameter to No. 3. Scroll to the Subnet Mask parameter, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey, and then press the **Save** softkey.

Table 5-1 Network Configuration Menu Parameters (continued)

Parameter	Description	To Change
TFTP Server	IP address or URL of the TFTP server from which a phone obtains a profile. Required if the DHCP server does not provide the TFTP server address. If you set the Alternate TFTP parameter to Yes, you must enter a non-zero value for the TFTP Server parameter.	1. Unlock configuration parameters. 2. Set the TFTP Enabled parameter to Yes. 3. Set the Alternate TFTP parameter to Yes. 4. Scroll to the TFTP Server parameter, press the **Edit** softkey, and then enter a new TFTP server IP address or URL. 5. Press the **Validate** softkey, and then press the **Save** softkey.
Default Router	IP address of the network gateway used by the phone. You can use this parameter to assign this address if DHCP does not provide it. If you assign a network gateway address with this parameter, you must also assign an IP address and a subnet mask for the phone. See the IP Address and the Subnet Mask parameters in this table.	1. Unlock configuration parameters. 2. Set the DHCP Enabled parameter to No. 3. Scroll to the Default Router parameter, press the **Edit** softkey, and then enter a new network gateway IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey.
DNS Server 1, DNS Server 2	IP addresses of the Primary Domain Name System (DNS) server (DNS Server 1) and secondary DNS server (DNS Server 2) used by the phone.	1. Unlock configuration parameters. 2. Set the Alternate DNS parameter to Yes. 3. Scroll to the DNS Server 1 parameter or the DNS Server 2 parameter, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey.

Table 5-1 Network Configuration Menu Parameters (continued)

Parameter	Description	To Change
NTP Server 1, NTP Server 2	IP addresses of the Primary Network Time Protocol (NTP) server (NTP Server 1) and secondary NTP server (NTP Server 2) used by the phone.	1. Unlock configuration parameters. 2. Set the Alternate NTP parameter to Yes. 3. Scroll to the NTP Server 1 parameter or the NTP Server 2 parameter, press the **Edit** softkey, and then enter a new NTP server IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey.
Time Zone	Offset to apply to the Greenwich Mean Time (GMT) returned by an NTP server to determine local time (to use for Call ID display, for example). Local time is generated as follows: • Local time = GMT + Time Zone, if Time Zone <= 12. • Local time = GMT + Time Zone – 25, if Time Zone > 12. For example, Time Zone = 17 for Pacific Standard Time. **Note** You must update this parameter manually when daylight savings time goes into effect and ends.	1. Unlock configuration parameters. 2. Scroll to the Time Zone parameter, press the **Edit** softkey, and then enter a new time zone offset value. 3. Press the **Validate** softkey, and then press the **Save** softkey.

Table 5-1 Network Configuration Menu Parameters (continued)

Parameter	Description	To Change
Operational VLAN Id	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member. If the phone has not received an auxiliary VLAN, this parameter indicates the Administrative VLAN. If neither the auxiliary VLAN nor the Administrative VLAN are configured, this parameter is blank.	The phone obtains its Operational VLAN Id via Cisco Discovery Protocol (CDP) from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN Id parameter.
Admin. VLAN Id	Auxiliary VLAN in which the phone is a member. Overrides the value specified by the Operation VLAN Id parameter.	1. Unlock configuration parameters. 2. Scroll to the Admin. VLAN Id parameter, press the **Edit** softkey, and then enter a new Admin VLAN value. 3. Press the **Validate** softkey, and then press the **Save** softkey.
VLAN Enabled	Indicates whether VLAN is enabled for the phone.	1. Unlock configuration parameters. 2. Scroll to the VLAN Enabled parameter and press the **No** softkey to disable VLAN, or press the **Yes** softkey to enable VLAN. 3. Press the **Save** softkey.

Table 5-1 Network Configuration Menu Parameters (continued)

Parameter	Description	To Change
CDP Enabled	Indicates whether Cisco Discovery Protocol (CDP) is enabled for the phone. CDP allows the phone to be discovered by the CiscoWorks network management system. For more information about CiscoWorks2000, refer to the documentation available at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm	1. Unlock configuration parameters. 2. Scroll to the CDP Enabled parameter and press the **No** softkey to disable CDP, or press the **Yes** softkey to enable CDP. 3. Press the **Save** softkey.
DHCP Enabled	Specifies whether to use the DHCP server to obtain information such as its IP address, its subnet mask, and the IP addresses of the network gateway and the DNS, NTP, and TFTP servers. If this parameter is 0, you must manually specify the IP address of the phone, and the subnet mask and the network gateway (default router) used by the phone. See the "Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G" section on page 3-9 for more information.	1. Unlock configuration parameters. 2. Scroll to the DHCP Enabled parameter and press the **No** softkey to disable DHCP, or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.

Table 5-1 Network Configuration Menu Parameters (continued)

Parameter	Description	To Change
TFTP Enabled	Enables or disables downloading of a profile from a TFTP server. If you set this parameter to Yes and subsequently make changes using the web interface, you must set this parameter to No before saving those changes; otherwise, the changes will be overwritten by the profile obtained from a TFTP server. If you set this parameter to Yes and do not specify a TFTP server, the phone will use the TFTP IP address or URL obtained from the DHCP server to contact the TFTP server. If you set this parameter to Yes, set the Alternate TFTP parameter to Yes, and specify a value for the TFTP Server parameter, the phone will use the server that you specify.	1. Unlock configuration parameters. 2. Scroll to the TFTP Enabled parameter and press the **No** softkey to disable TFTP, or press the **Yes** softkey to enable TFTP. 3. Press the **Save** softkey.
Alternate TFTP	Indicates whether the phone obtains the IP address or URL of the TFTP server from the DHCP server (No) or uses the IP address or URL specified by the TFTP Server parameter (Yes). If you set the Alternate TFTP server to Yes, you must specify a value for the TFTP Server parameter.	1. Unlock configuration parameters. 2. Scroll to the Alternate TFTP parameter and press the **Yes** softkey if the phone should use an alternative TFTP server. Press the **No** softkey otherwise. 3. Press the **Save** softkey.

Table 5-1 Network Configuration Menu Parameters (continued)

Parameter	Description	To Change
Alternate DNS	Indicates whether the phone obtains the IP address of the DNS server from the DHCP server (No) or uses the IP addresses specified by the DNS Server 1 and, optionally, the DNS Server 2 parameters (Yes). If you set the Alternate DNS server to Yes, you must specify a value for the DNS Server 1 parameter. You may also specify a value for the DNS Server 2 parameter.	1. Unlock configuration parameters. 2. Scroll to the Alternate DNS parameter and press the **Yes** softkey if the phone should use an alternative DNS. Press the **No** softkey otherwise. 3. Press the **Save** softkey.
Alternate NTP	Indicates whether the phone obtains the IP address of the NTP server from the DHCP server (No) or uses the IP addresses specified by the NTP Server 1 and, optionally, the NTP Server 2 parameters (Yes). If you set the Alternate NTP server to Yes, you must specify a value for the NTP Server 1 parameter. You may also specify a value for the NTP Server 2 parameter.	1. Unlock configuration parameters. 2. Scroll to the Alternate NTP parameter and press the **Yes** softkey if the phone should use an alternative NTP server. Press the **No** softkey otherwise. 3. Press the **Save** softkey.
Alternate Domain	Indicates whether the phone is using an alternative domain name. If you set this parameter to Yes, you must specify a value for the Domain Name parameter.	1. Unlock configuration parameters. 2. Scroll to the Alternate Domain parameter and press the **Yes** softkey if the phone should use an alternative domain name. Press the **No** softkey otherwise. 3. Press the **Save** softkey.

Table 5-1 Network Configuration Menu Parameters (continued)

Parameter	Description	To Change
Profile Encrypt Key	Specifies an encryption key used to decrypt the profile that the phone downloads from the TFTP server. For more information about encryption keys, see "Using Encryption" section on page 6-15.	1. Unlock configuration parameters. 2. Scroll to the Profile Encryption Key parameter, press the **Edit** softkey, and then enter a new encryption key. 3. Press the **Validate** softkey, and then press the **Save** softkey.
Erase Configuration	Changes these settings to their default values: Network Configuration menu settings (including password), SIP Configuration menu settings, Call Preferences menu settings, volume settings, and contrast settings.	1. Unlock configuration parameters. 2. Scroll to the Erase Configuration parameter, press the **Yes** softkey, and then press the **Save** softkey.

SIP Configuration Menu

The SIP Configuration menu lets you configure a variety of SIP signaling parameters. Table 5-2 describes these parameters and explains how to change them.

Note The **Edit**, **Yes**, or **No** softkeys for changing SIP configuration parameters appear only if parameters are unlocked as described in the "Unlocking and Locking Configuration Parameters" section on page 5-4. For information about the keys you can use to edit parameters, see the "Editing Parameter Values" section on page 5-5.

Table 5-2 SIP Configuration Menu Parameters

Parameter	Description	To Change
SIP Proxy	IP address or URL of the SIP proxy server used by the phone.	1. Unlock configuration parameters. 2. Scroll to the SIP Proxy parameter, press the **Edit** softkey, and then enter the IP address or URL of a SIP proxy server. 3. Press the **Accept** softkey, and then press the **Save** softkey.
User ID	User ID for registration and authentication of the phone.	1. Unlock configuration parameters. 2. Scroll to the User ID parameter, press the **Edit** softkey, and then enter a user ID. 3. Press the **Accept** softkey, and then press the **Save** softkey.
Password	Password for registration and authentication of the phone.	1. Unlock configuration parameters. 2. Scroll to the Password parameter, press the **Edit** softkey, and then enter a Password. 3. Press the **Accept** softkey, and then press the **Save** softkey.
Use Login ID	Indicates whether to use the value specified with the Login ID parameter instead of the value specified with the User ID parameter for registration and authentication of the phone.	1. Unlock configuration parameters. 2. Scroll to the Use Login ID parameter, and then press the **Yes** softkey to use the value specified with the Login ID parameter for registration and authentication. 3. Press the **Save** softkey.
Login ID	Alternate ID used for authentication of the phone.	1. Unlock configuration parameters. 2. Set the Use Login ID parameter to Yes. 3. Scroll to the Login ID parameter, press the **Edit** softkey, and then enter a login ID. 4. Press the **Accept** softkey, and then press the **Save** softkey.

Table 5-2 SIP Configuration Menu Parameters (continued)

Parameter	Description	To Change
Local SIP Port	Port where the phone listens for incoming requests and sends outgoing requests.	1. Unlock configuration parameters. 2. Scroll to the Local SIP Port parameter, press the **Edit** softkey, and then enter a SIP port from 5060 to 65535. 3. Press the **Accept** softkey, and then press the **Save** softkey.
Local RTP Port	Port from which the phone transmits and receives media streams.	1. Unlock configuration parameters. 2. Scroll to the Local RTP Port parameter, press the **Edit** softkey, and then enter a SIP port, which must be an even number from 0 to 65535. 3. Press the **Accept** softkey, and then press the **Save** softkey.
Backup Proxy Timeout	Timeout, in seconds, for switching from backup proxy server to primary proxy server. The value can range from 0 to 4294967295.	1. Unlock configuration parameters. 2. Scroll to the Backup Proxy Timeout parameter, press the **Edit** softkey, and then enter a timeout value. 3. Press the **Accept** softkey, and then press the **Save** softkey.
Outbound Proxy	IP address or URL of the SIP outbound proxy server used by the phone.	1. Unlock configuration parameters. 2. Scroll to the Outbound Proxy parameter, press the **Edit** softkey, and then enter the IP address or URL of the outbound proxy server. 3. Press the **Accept** softkey, and then press the **Save** softkey.

Table 5-2 SIP Configuration Menu Parameters (continued)

Parameter	Description	To Change
Register Expires	SIP registration interval, in seconds, between each registration renewal to the SIP proxy server. The value can range from 1 to 86400.	1. Unlock configuration parameters. 2. Scroll to the Register Expires parameter, press the **Edit** softkey, and then enter the SIP registration interval. 3. Press the **Accept** softkey, and then press the **Save** softkey.
Register with Proxy	Indicates whether to enable SIP registration. This parameter is ignored if a SIP proxy server is not specified.	1. Unlock configuration parameters. 2. Scroll to the Register with Proxy and press the **Yes** softkey to enable SIP registration, or press the **No** softkey to disable SIP registration. 3. Press the **Save** softkey.
NAT WAN IP Address	External Network Address Translation (NAT) IP address where other SIP user agents can communicate with the phone.	1. Unlock configuration parameters. 2. Scroll to the NAT WAN IP Address parameter, press the **Edit** softkey, and then enter the NAT IP address. 3. Press the **Accept** softkey, and then press the **Save** softkey.

Model Information Menu

The Model Information menu provides information that can assist with troubleshooting the phone.

The Model Information menu shows the following information:

- Model Number—The model number of the phone.
- MAC Address—The MAC address of the phone.
- App Load ID—Identifier of the firmware running on the phone.
- Boot Load ID—Identifier of the factory-installed load running on the phone.
- Serial Number—Serial number of the phone.

Status Menu

The Status menu contains the following options, which provide information about the phone and its operation:

- Status Messages—Reserved for future use.
- Network Statistics—Displays Ethernet traffic statistics.
- Firmware Versions—Displays this information about the software and firmware running on the phone:
  - Application Load ID—Identifier of the firmware.
  - Boot Load ID—Identifier of the factory-installed load.
  - Version—Software version number.

To access the Status menu, choose **Status** from the Settings menu.

Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server

This chapter explains how to configure the Cisco IP Phone using a Trivial File Transfer Protocol (TFTP) server. This configuration method is useful when you have many Cisco IP Phones because you can use a TFTP server for remote, batch configuration of the phones. The TFTP server can also host one unique configuration file for each phone.

To obtain configuration information from a TFTP server, a phone downloads a configuration file, called a *profile*. A profile contains various parameters and values for phone and network settings.

You can also configure many parameters for a Cisco IP Phone by using the configuration menus on a phone and by using the phone's web page. For more information, see Chapter 5, "Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus," and Chapter 7, "Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages."

For an explanation of the parameters that you can use in a profile, see Chapter 8, "Profile and Web Page Parameters and Defaults."

For a list of the configurable parameters on the phone menus and their equivalent profile and web page parameters, see Appendix B, "Phone Menu, Web Page, and Profile Equivalent Parameters."

For an overview of configuring the Cisco IP Phone, see Chapter 3, "Configuring the Cisco IP Phone Models 7905G and 7912G for SIP."

If you are not using a Dynamic Host Configuration Protocol (DHCP) server, you must manually define IP addresses, subnet masks, and gateways for the phones before you can access profiles. For more information, see the "Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G" section on page 3-9.

Note Parameter values that you set in a profile will overwrite values that you set from a phone's Network Configuration menu, its SIP Configuration menu, or its web page.

This chapter includes the following topics:

- Using Profiles with TFTP Configuration, page 6-2
- Setting Up the TFTP Server with Cisco IP Phone Software, page 6-4
- Configuring the Cisco IP Phone to Obtain its Configuration File from the TFTP Server, page 6-5
- Creating or Updating a Profile, page 6-9
- Using Encryption, page 6-15
- Refreshing or Resetting the Cisco IP Phone, page 6-17

Using Profiles with TFTP Configuration

After the Cisco IP Phone has been configured with the minimum settings as explained in the "Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G" section on page 3-9, you can configure many additional parameters using a file called a *profile*. A profile is stored on the TFTP server and contains a list of tag, length, and value triplets (TLVs) that represent some of the configuration parameters for the Cisco IP Phone. You can edit a text version of a profile file and then convert it to a binary file for the phone to download.

TFTP configuration works as follows:

1. The Cisco IP Phone model 7905G will try to download the profile ld*xxxxxxxxxxxx* from the TFTP server. The Cisco IP Phone model 7912G will try to download the profile gk*xxxxxxxxxxxx* from the TFTP server. In these file names, each *xx* is the two-digit lowercase hexadecimal representation of each integer in the phone's MAC address.
2. If the ld*xxxxxxxxxxxx* or the gk*xxxxxxxxxxxx* profile does not exist, the Cisco IP Phone 7905G will try to download profile lddefault.cfg, and the Cisco IP Phone 7912G will try to download profile gkdefault.cfg

Use the ld*xxxxxxxxxxxx* or the gk*xxxxxxxxxxxx* profile to configure a particular Cisco IP Phone. Use the lddefault.cfg or the gkdefault.cfg profile to simultaneously configure multiple phones of the same model with the same information.

Parameter values in a profile will overwrite any values configured through the web or through the phone configuration menus when the phone powers up or refreshes.

Note If you name a profile something other than ld*xxxxxxxxxxxx* or gk*xxxxxxxxxxxx*, you must configure DHCP with the name of the profile or else the phone will not recognize it.

Related Topics

- Setting Up the TFTP Server with Cisco IP Phone Software, page 6-4
- Configuring the Cisco IP Phone to Obtain its Configuration File from the TFTP Server, page 6-5
- Creating or Updating a Profile, page 6-9
- Using Encryption, page 6-15
- Refreshing or Resetting the Cisco IP Phone, page 6-17

Setting Up the TFTP Server with Cisco IP Phone Software

Before you can use a TFTP server to configure a Cisco IP Phone, the firmware image that you are using for the phone must exist on the TFTP server. To obtain the correct firmware image and install it on the TFTP server, perform the following steps.

Note You must be a registered Cisco.com user to download the firmware image.

Procedure

Step 1 Go to the following URL:

http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Step 2 Download the zip file that contains the software for the applicable release and firmware image you are using. The contents of each file are described next to the file name.

Note A firmware image can contain a signature that allows a phone to verify the authenticity of the image. A firmware image with such a signature has the extension .sbin. A firmware image without such a signature has the extension .zup. For the Cisco IP Phone 7905G, you should obtain both the .sbin and the .zup versions of a firmware image. After a phone upgrades to a .zup firmware image, it will request .sbin firmware images for future firmware upgrades. If a phone upgrades to a .zup firmware image released after March 26, 2003, the phone cannot be upgraded or downgraded to any other .zup firmware image. In addition, a phone cannot be downgraded from a .sbin firmware image to a .zup firmware image. (The Cisco IP Phone 7912G is distributed with a .sbin firmware image.)

Step 3 Extract the firmware files onto the TFTP server.

This server should be the same one that will contain the binary profile file that you create as described in this chapter.

Related Topics

- Using Profiles with TFTP Configuration, page 6-2
- Configuring the Cisco IP Phone to Obtain its Configuration File from the TFTP Server, page 6-5
- Creating or Updating a Profile, page 6-9
- Using Encryption, page 6-15
- Refreshing or Resetting the Cisco IP Phone, page 6-17

Configuring the Cisco IP Phone to Obtain its Configuration File from the TFTP Server

This section describes the following ways in which the Cisco IP Phone can contact the TFTP server to obtain its profile:

- Using a DHCP Server, page 6-5
  - The phone contacts the DHCP server, which provides the IP address of the TFTP server
  - The phone uses the DHCP server but the DHCP server does not know about the TFTP server
- Without Using a DHCP Server, page 6-8

Using a DHCP Server

Configuration settings for a DHCP server vary depending on whether the DHCP server is under the control of the Cisco IP Phone system administrator or the service provider. The simplest configuration is when the DHCP server is under the control of the Cisco IP Phone administrator, in which case the DHCP server provides the IP address of the TFTP server. Depending on who controls the DHCP server, follow the applicable configuration procedure:

- If the DHCP Server is Under Control of the Cisco IP Phone Administrator, page 6-6
- If the DHCP Server is not Under the Control of the Cisco IP Phone Administrator, page 6-7

This section also includes this topic:

- Other DHCP Options You Can Set, page 6-7

The procedures in the following sections instruct you to set various parameter values using a phone's configuration menus or web page. For information about phone menu configuration and parameters, see Chapter 5, "Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus." For information about web page configuration, see Chapter 7, "Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages." For information about web page parameters, see the "Network Parameters" section on page 8-2.

You can configure parameters through configuration menus on a phone without first obtaining network connectivity for the phone. If you want to configure a parameter using the phone's web page, you first must obtain network connectivity by statically configuring IP with the settings as explained in the "Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G" section on page 3-9.

If the DHCP Server is Under Control of the Cisco IP Phone Administrator

If you as the Cisco IP Phone administrator control the DHCP server, follow these steps to make appropriate DHCP server configuration settings:

Procedure

Step 1 On the DHCP server, set one of the following options:

- DHCP option 150 (TFTP server IP address)
- Standard DHCP option 66 (TFTP server name)

If you use DHCP option 150, the Cisco IP Phone will ignore DHCP option 66. However, if you use DHCP option 66, you must turn off DHCP option 150 or set its value to 0.

Note You can turn off the DHCP option 150 request by using OpFlags parameter. See the "Network Parameters" section on page 8-2.

Step 2 Make sure to use these default values for the following configuration parameters:

- TftpURL=0
- UseTftp=1
- DHCP=1

After you complete these steps, the Cisco IP Phone will contact the DHCP server for the IP address of the TFTP server that contains the Cisco IP Phone profile.

If the DHCP Server is not Under the Control of the Cisco IP Phone Administrator

If you as the Cisco IP Phone adminstrator do not control the DHCP server, you must manually configure the URL of the TFTP server.

Procedure

Step 1 Set the TFTP Server parameter (on the phone's Network Configuration menu) or the TftpURL parameter (on the phone's web page) to the IP address or the URL of the TFTP server.

Step 2 Make sure that the DHCP Enabled parameter on the phone's Network Configuration menu is set to Yes (the default value) or that the Dhcp parameter on the phone's web page is set to 1 (the default value).

Step 3 Make sure that the TFTP Enabled parameter on the phone's Network Configuration menu is set to Yes (the default value) or that the UseTftp parameter on the phone's web page is set to 1 (the default value).

After you complete these steps, the Cisco IP Phone will contact the manually-configured TFTP server that contains the phone's profile.

Other DHCP Options You Can Set

The DHCP server can use option 60 (DHCP_VENDOR_CLASS_ID) to identify Cisco IP Phone models 7905G and 7912G devices on the network. If specific phones with specific MAC addresses need to download a TFTP file, the file name

can be set in the bootfile name field of the DHCP header. This field is limited to 31 characters, even though the DHCP specification allows for a longer bootfile name.

You can configure the following phone configuration parameters using DHCP:

- Client IP address
- DHCP option 1: Client subnet mask
- DHCP option 3: Routers on the client's subnet
- DHCP option 6: Domain Name System (DNS) server (up to two)
- DHCP option 42: Network Time Protocol (NTP) server (up to two)
- DHCP option 66: TFTP server

The values for DNS server, NTP server, and TFTP server can be overwritten by values in the corresponding parameters in the phone profile (DNS1IP, DNS2IP, NTPIP, AltNTPIP, and TftpURL). If these parameters are not set to 0, their values are used in place of those corresponding values that are supplied by the DHCP options.

Without Using a DHCP Server

If you are not using a DHCP server in your environment but are still using a TFTP server to obtain the Cisco IP Phone profile, follow these steps so that the Cisco IP Phone can contact the TFTP server without using DHCP:

Procedure

Step 1 Set the DHCP Enabled parameter on the phone's Network Configuration menu to No or set the Dhcp parameter on the phone's web page to 0.

Step 2 Set the TFTP Enabled parameter on the phone's Network Configuration menu to Yes or set the UseTftp parameter on the phone's web page to 1.

Step 3 Set the TFTP Server parameter on the phone's Network Configuration menu to the IP address or the URL of the TFTP server or set the TftpURL parameter on the phone's web page to the IP address or the URL of the TFTP server.

Step 4 If you have done already done so, statically configure the following parameters using the phone's Network Configuration menu. These parameters are required for the phone to obtain network connectivity:

- IP Address
- Network gateway (default router)
- Subnet Mask

You may also provide other parameters that are normally supplied by DHCP by configuring their values. These parameters are:

- DNS Server 1
- DNS Server 2
- NTP Server 1
- NTP Server 2
- Domain Name

After you complete these steps, the Cisco IP Phone will be able to contact the TFTP server (without using DHCP) that will contain the configuration file for the phone.

Related Topics

- Using Profiles with TFTP Configuration, page 6-2
- Setting Up the TFTP Server with Cisco IP Phone Software, page 6-4
- Creating or Updating a Profile, page 6-9
- Using Encryption, page 6-15
- Refreshing or Resetting the Cisco IP Phone, page 6-17

Creating or Updating a Profile

The profile from which a Cisco IP Phone obtains information is a binary file. However, when you create or edit a profile, you work with a text version of the file, then create a binary version from the text file. Before you can create a binary profile, you will need the cfgfmt.exe tool, which converts a text profile file to binary format.

The cfgfmt.exe tool requires a parameter tag file, which specifies the type and size of each parameter. By default, the cfgfmt.exe tool looks in the folder from which you run the tool for a parameter tag file named ptag.dat. Cisco recommends that

you use the parameter tag file called sip_ptag.dat, which Cisco provides. You can rename sip_ptag.dat to ptag.dat before you run the cfgfmt.exe tool, or you can use the cfgfmt.exe tool -t option to specify the file name sip_ptag.dat. (See the "Creating a Phone-Specific Profile" section on page 6-11 or the "Creating a Default Profile" section on page 6-13 for more information.)

The cfgfmt.exe tool and the sip_ptag.dat file are bundled with the Cisco IP Phone software.

This section includes these topics:

- Profile Conventions, page 6-10
- Creating a Phone-Specific Profile, page 6-11
- Creating a Default Profile, page 6-13

Related Topics

- Using Profiles with TFTP Configuration, page 6-2
- Setting Up the TFTP Server with Cisco IP Phone Software, page 6-4
- Configuring the Cisco IP Phone to Obtain its Configuration File from the TFTP Server, page 6-5
- Using Encryption, page 6-15
- Refreshing or Resetting the Cisco IP Phone, page 6-17

Profile Conventions

A text profile file must conform to the following conventions:

- The characters **#txt** must appear at the beginning of the first line of the file so that the formatting tool, cfgfmt.exe, will treat the file as a text file.
- A pound sign (#) must appear at the beginning of a line that is a comment.
- Parameter/value pairs must be in the form *parameter*:*value*, where *parameter* is the exact name of the parameter and *value* is a valid value.
- Each parameter/value pair must appear on its own line.
- All parameter/value pairs are optional, but the Cisco IP Phone might not function properly if some values are missing.

- A parameter value must be one of the following types:
  - Alphanumeric string
  - Numeric digit string
  - Array of short integers
  - IP address (for example, 192.168.2.170)
  - Extended IP address (IP address with port; for example, 192.168.2.170.9001)
  - Boolean (1 or 0)
  - Bitmap (unsigned hexadecimal integer, for specifying bits in 32-bit integer)
  - Integer (32-bit integer)

Related Topics

- Creating a Phone-Specific Profile, page 6-11
- Creating a Default Profile, page 6-13
- Using Encryption, page 6-15
- Refreshing or Resetting the Cisco IP Phone, page 6-17

Creating a Phone-Specific Profile

The following steps explain how to create a phone-specific profile and how to convert it to binary format.

When you create a phone-specific profile, you can use the sipexample.txt file as a template. The sipexample.txt file is bundled with the Cisco IP Phone software contains default values for parameters.

Tip If you will create several unique profiles for various Cisco IP Phones, copy the sipexample.txt file (or another existing profile) to a file with a meaningful name, such as common.txt. Edit the new file, configure parameters and values that are common to all of the phones, and save this file. Then, when you create a unique profile for a phone, you can use the Include parameter to include common parameters from the common file you just created. This way, you just need to

configure parameters in the unique profile that are specific to a phone. For more information about the Include parameter, see the "Profile Parameters" section on page 8-26.

Procedure

Step 1 Use a text editor to open the sipexample.txt file or to open another existing text profile.

Step 2 Edit or enter parameter:value pairs in the profile as needed.

For an explanation of parameters that you can include in a profile, see Chapter 8, "Profile and Web Page Parameters and Defaults."

Note If you use the Include parameter, Cisco recommends that it be the first parameter in a text profile file. Any parameters in a text profile that come before an include statement will be overwritten with values from the same parameters, if they exist, in a common profile.

Step 3 Save the file and name it as follows, where each *xx* is the two-digit lowercase hexadecimal representation of each integer in the phone's MAC address. A file name must contain exactly 14 characters.

- File name for the Cisco IP Phone 7905G: ld*xxxxxxxxxxxx*.txt
- File name for the Cisco IP Phone 7912G: gk*xxxxxxxxxxxx*.txt

You can determine the MAC address of a phone from the MAC Address parameter in the Network Configuration menu or the Device Information area in the phone's web page.

Step 4 Open a command window and type the following command to generate the binary profile file from the text file:

```
cfgfmt [-eRC4Password] [-tpTagFile] input-text-file output-binary-file
```

where:

- *RC4Password* is the optional RC4 key, up to eight alphanumeric characters, to encrypt the binary profile that is generated by the cfgfmt tool. For more information, see the "Using Encryption" section on page 6-15.

- *pTagFile* is an optional path and file name (or file name only) of the parameter tag file. Use this option if the parameter tag file is not in the folder from which you are running the cfgfmt.exe tool, and if the parameter tag file is not named ptag.dat.
- *input-text-file* is the name of the text version of the profile file. Make sure to include any extension, such as .txt.
- *output-binary-file* is the name of the binary file that the Cisco IP Phone uses as the TFTP configuration profile file. Specify the file name as follows, as follows, where each *xx* is the two-digit lowercase hexadecimal representation of each integer in the phone's MAC address. The file name must contain exactly 14 characters.
  - File name for the Cisco IP Phone 7905G: ld*xxxxxxxxxxxx*
  - File name for the Cisco IP Phone 7912G: gk*xxxxxxxxxxxx*

Step 5 Put the binary file in the root directory on the TFTP server

When the Cisco IP Phone powers up or refreshes, it will retrieve its unique configuration file from the TFTP server.

If you want to refresh the phone immediately, see the "Refreshing or Resetting the Cisco IP Phone" section on page 6-17.) If you do not perform a refresh procedure, the phone will update its configuration the next time it contacts the TFTP server.

Related Topics

- Creating a Default Profile, page 6-13
- Using Encryption, page 6-15
- Refreshing or Resetting the Cisco IP Phone, page 6-17

Creating a Default Profile

You can create a default profile, called lddefault.cfg for the Cisco IP Phone 7905G, or gkdefault.cfg for the Cisco IP Phone 7912G, that is common to all Cisco IP Phones of the same model. This profile is applied to a phone only if a phone-specific profile (ld*xxxxxxxxxxxx* or gk*xxxxxxxxxxxx*) does not exist for the phone on the TFTP server when the phone powers up.

The following steps explain how to create a default profile, how to convert it to binary format, and how to store it on the TFTP server so that the Cisco IP Phone will download it during the boot-up process:

Procedure

Step 1 Use a text editor to open the sipexample.txt file or to open another existing text profile.

Step 2 Edit or enter parameter:value pairs in the profile as needed.

For an explanation of parameters that you can include in a profile, see Chapter 8, "Profile and Web Page Parameters and Defaults."

Step 3 Save the file and name it as follows:

- File name for the Cisco IP Phone 7905G: lddefault.txt
- File name for the Cisco IP Phone 7912G: gkdefault.txt

Step 4 Open a command window and type the following command to generate the binary profile file from the text file:

```
cfgfmt [-eRC4Password] [-tpTagFile] input-text-file {lddefault.cfg |
gkdefault.cfg}
```

where:

- *RC4Password* is the optional RC4 key, up to eight alphanumeric characters, to encrypt the binary profile that is generated by the cfgfmt tool. For more information, see the "Using Encryption" section on page 6-15.
- *pTagFile* is an optional path and file name (or file name only) of the parameter tag file. Use this option if the parameter tag file is not in the folder from which you are running the cfgfmt.exe tool, and if the parameter tag file is not named ptag.dat.
- *input-text-file* is the name of the text version of the profile file. Make sure to include any extension, such as .txt.

Step 5 Put the binary file in the root directory on the TFTP server

When the Cisco IP Phone powers up or refreshes, the phone will download this file as its profile file unless it first finds a phone-specific profile.

If you want to refresh the phone immediately, see the "Refreshing or Resetting the Cisco IP Phone" section on page 6-17.) If you do not perform a refresh procedure, the phone will update its configuration the next time it contacts the TFTP server.

Related Topics

- Creating a Phone-Specific Profile, page 6-11
- Using Encryption, page 6-15
- Refreshing or Resetting the Cisco IP Phone, page 6-17

Using Encryption

The EncryptKey parameter encrypts binary files that are transferred over TFTP. You can change this key for each Cisco IP Phone so that only one specific phone can decode the information.

By default, the phone-specific profile is not encrypted. If encryption is required, you must manually configure the phone with the encryption key. Use either the Profile Encrypt Key parameter on the phone's Network Configuration menu or the EncryptKey key parameter in the Network Parameters area on a phone's web page.

Note Because the factory-fresh phone cannot accept encrypted configuration files, the first unencrypted file, if intercepted, can easily be read. (You would still have to know the data structure format in order to decode the binary information from the unencrypted file.) Therefore, the new encryption key in the unencrypted file can be compromised.

When the EncryptKey parameter is set to a nonzero value, the Cisco IP Phone assumes that the binary configuration file on the TFTP server is to be encrypted with this key by means of the RC4 cipher algorithm. The phone will use this key to decrypt the configuration file.

The EncryptKey parameter or the profile Encrypt Key parameter and the encryption key used in the cfgfmt tool command syntax must match.

The cfgfmt.exe syntax affects how the EncryptKey parameter is used, as shown in the following examples. In these examples, input_text is the ld*xxxxxxxxxxxx*.txt or the gk*xxxxxxxxxxxx*.txt file that you will convert to a binary profile, output_binary is the binary ld*xxxxxxxxxxxx* or gk*xxxxxxxxxxxx* file, and *Secret* is the encryption key.

Syntax examples

- `cfgfmt input-text-file output-binary-file`

  If input-text-file sets the EncryptKey parameter to 0, then output-binary-file is not encrypted. If input-text-file sets EncryptKey to a non-zero value, then output-binary-file is encrypted with that value.

- `cfgfmt -eSecret input-text-file output-binary-file`

  If the EncryptKey parameter has the value of 0 or is not included in input-text-file, the *Secret* is used to encrypt the output-binary-file. If input-text-file sets the EncryptKey parameter to a nonzero value and the -e option is used, then output-binary-file is encrypted with the EncryptKey parameter set in input-text-file and *Secret* is ignored.

- `cfgfmt -E input-text-file output-binary-file`

  The -E (uppercase) option means that any value specified for the EncryptKey parameter in input-text-file is ignored. However, because *Secret* is not specified in this example, output-binary-file is not encrypted. Nevertheless, the EncryptKey parameter and its value, if specified in input-file-text, will be included in output-binary-file for possible encryption at a later time.

- `cfgfmt -E -eSecret input-text-file output-binary-file`

  The -E (uppercase) option means that any value specified for the EncryptKey parameter in input-text-file is ignored and the output-binary-file is encrypted with the *Secret* key. However, the EncryptKey parameter and its value, if specified in input-text-file, will be included in output-binary-file.

Refreshing or Resetting the Cisco IP Phone

When you make configuration changes to a Cisco IP Phone profile, you can refresh or reset the Cisco IP Phone for these configuration changes to immediately take effect. If you do not refresh or reset the phone, the configuration changes will take effect the next time the phone contacts the TFTP server, which occurs based on the configured value of the CfgInterval parameter.

A refresh procedure will update a phone with the current profile. A reset procedure will update a phone with the current profile and will power-down and power-up the phone. A reset is not necessary if your only goal is to update a phone's profile.

Note You use bits 8 and 0 of the OpFlags parameter prevent end users from refreshing or resetting a phone. See the "Network Parameters" section on page 8-2 for more information.

This section includes the following topics:

- Refreshing the Cisco IP Phone, page 6-17
- Resetting the Cisco IP Phone, page 6-17

Refreshing the Cisco IP Phone

To refresh the Cisco IP Phone, enter the following command from your web browser:

http://<*ipaddress*>/refresh

where ***ipaddress*** is the IP address of the Cisco IP Phone that you are refreshing.

Resetting the Cisco IP Phone

To reset the Cisco IP Phone, enter the following command from your web browser:

http://<*ipaddress*>/reset

where ***ipaddress*** is the IP address of the Cisco IP Phone that you are resetting.

Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages

Each phone has a web page from which you can view and update many device and network parameter values. You can also use the web page to obtain a variety of statistical and operational information about the phone. This chapter describes how use a phone's web page to configure parameters and to obtain information.

You can also configure many parameters for a Cisco IP Phone using the configuration menus on the phone and using profiles. For more information, see Chapter 5, "Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus," and Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server."

For an explanation of the parameters that you can configure from a phone's web page, see Chapter 8, "Profile and Web Page Parameters and Defaults."

For a list of the configurable parameters on the phone menus and their equivalent web page and profile parameters, see Appendix B, "Phone Menu, Web Page, and Profile Equivalent Parameters."

If you are not using a Dynamic Host Configuration Protocol (DHCP) server, you must manually configure the IP address of the phone, the subnet mask used by the phone, and the network gateway (default router) IP address for the phone before you can access the web page for the phone. For more information, see the "Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G" section on page 3-9.

Note If you configure a phone using a TFTP server, parameter values in a profile will overwrite values that you set from the phone's web page for the same parameters.

This chapter includes the following topics:

- Accessing a Phone's Web Page, page 7-2
- Viewing Statistical and Operational Information, page 7-4

Accessing a Phone's Web Page

You can display and configure device and network information for a Cisco IP Phone through the phone's web page. You can access the web page using any graphically capable web browser.

Note Cisco recommends that you take care to prevent unauthorized access to a phone's web page and that you increase security by setting a password using the UIPassword parameter in the phone's profile. For more information about this parameter, see the "Profile Parameters" section on page 8-26. For security reasons, Cisco also recommends that you do not use the web interface over the public network. Disable the web interface by setting the OpFlags parameter bit 7 (mask 0x80) to 1 before the phone leaves the service-provider site. After the parameter bit is set, limited configuration can be done through the configuration menus on a phone and full configuration can be done through the TFTP server.

To access the web page for a Cisco IP Phone, perform the following steps.

If you want to edit parameters in the Network Parameters, SIP Parameters, Call Preferences, Tone Parameters, or Audio Parameters areas, you must first set up a password with the UIPassword parameter in the profile. If you do not set up a password, you will be able to view information in these areas, but you will not be able to change parameters, and **Apply** will not be available.

Procedure

Step 1 Open a web browser and enter the URL of the web page for the phone as follows:

http://*IP_address*/dev

where *IP_address* is the IP address of the Cisco IP Phone.

You can determine the IP address on a phone by pressing the **Menu** button, choosing **Settings > Network Configuration**, and then scrolling to the IP Address option.

For example, the configuration page for a Cisco IP Phone with the IP address 192.168.3.225 is:

http://192.168.3.225/dev

Step 2 From the phone's web page, choose the hyperlink for the information that you want to display or configure:

- **Device Information**—Display only. For more information, see the "Device Information" section on page 7-4.
- **Network Configuration—**Display only. For more information, see the "Network Configuration" section on page 7-5.
- **Network Statistics**—Display only. For more information, see the "Network Statistics" section on page 7-6.
- **Device Logs**—Reserved for future use.
- **Network Parameters**—Configurable parameters. For more information, see the "Network Parameters" section on page 8-2.
- **SIP Parameters**—Configurable parameters. For more information, see the "SIP Parameters" section on page 8-9.
- **Call Preferences**—Configurable parameters. For more information, see the "Call Preference Parameters" section on page 8-13.
- **Tone Parameters**—Configurable parameters. For more information, see the "Tone Parameters" section on page 8-21.
- **Audio Parameters**—Configurable parameters. For more information, see the "Audio Parameters" section on page 8-24.

Step 3 If you selected **Network Parameters**, **SIP Parameters**, **Call Preferences**, **Tone Parameters**, or **Audio Parameters**, follow these steps:

a. If you have set up a password with the UIPassword parameter in the profile, enter the password in the UIPassword field, and then click **Apply**. (If you want to change the password, enter the new password in the two ChangeUIPassword fields before clicking **Apply**.)

b. Make changes to parameters as needed and click **Apply** to save your changes.

Step 4 Close your web browser.

Viewing Statistical and Operational Information

The following sections describe the information that you can obtain from a phone's web page. You can use this information to remotely monitor the operation of a phone and to assist with troubleshooting.

- Device Information, page 7-4
- Network Configuration, page 7-5
- Network Statistics, page 7-6

Device Information

Table 7-1 explains the fields displayed in the Device Information area of the Cisco IP Phone web page.

Note To access the Device Information area directly from a web browser, enter *ip_address*/**DeviceInformation**, where *ip_address* is the IP address of your Cisco IP Phone.

Table 7-1

Field	Explanation
MAC Address	Unique Media Access Control (MAC) address of the phone
Software Version	Version of the software running on the phone
Hardware Revision	Version of the phone hardware
Serial Number	Serial number of the phone
Product ID	Product identifier of the phone
H/W features	Reserved for future use
BTXML cards version	Version of the BTXML cards in the phone

Network Configuration

Table 7-2 explains the fields displayed in the Network Configuration area of the Cisco IP Phone web page.

Note To access the Network Configuration area from a web browser, enter *ip_address*/**NetworkConfiguration**, where *ip_address* is the IP address of your Cisco IP Phone.

Table 7-2

Field	Explanation
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server rather than a DHCP server
MAC Address	Unique Media Access Control (MAC) address of the phone

Table 7-2

Field	Explanation
Host Name	Unique host name of the phone
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides
IP Address	Internet Protocol (IP) address of the phone
Default Router	Network gateway used by the phone
Subnet Mask	Subnet mask used by the phone
TFTP Server 1	Trivial File Transfer Protocol (TFTP) server used by the phone
NTP Server 1	Primary Network Time Protocol (NTP) server used by the phone
NTP Server 2	Secondary NTP server used by the phone
DNS Server 1	Primary Domain Name System (DNS) server used by the phone
DNS Server 2	Secondary DNS server (DNS Server 2) used by the phone
Alt NTP Server 1	Primary alternate NTP server used by the phone
Alt NTP Server 2	Secondary alternate NTP server used by the phone

Network Statistics

Table 7-3 describes the fields displayed on the Network Statistics area of the Cisco IP Phone web page.

Note To access the Network Statistics area from a web browser, enter *ip_address*/**EthernetInformation**, where *ip_address* is the IP address of your Cisco IP Phone.

Table 7-3

Field	Explanation
Elapsed time	Time that has elapsed since the phone was last reset
Receive Packets	Number of packets that the phone has received during the elapsed time
Transmit Packets	Number of packets that the phone has transmitted during the elapsed time
Broadcast	Number of packets that the network has broadcast during the elapsed time
Multicast	Number of packets that the network has multicast during the elapsed time
Receive Errors	Number of receive errors that the phone has experienced during the elapsed time
Transmit Errors	Number of transmit errors that the phone has experienced during the elapsed time
Receive Overflow	Number of packet overflows that the phone has experienced during the elapsed time

Profile and Web Page Parameters and Defaults

This chapter describes the parameters that you can use to configure the Cisco IP Phone models 7905G and 7912G through a profile or through a phone's web page. These parameters are organized as follows:

- Network parameters—Controls various network-related activities of the phone.
- SIP parameters—Specifies SIP parameters of the phone.
- Call preferences—Controls various user features on the phone, and specifies which parameters appear and which options can be configured on a phone's Call Preference menu.
- Tone Parameters—Controls how the phone handles the various tones that it plays, and related options.
- Audio parameters—Controls how the phone handles various audio-related activities.
- Profile parameters—Parameters that are available only from the phone's profile.

You can also configure many parameters for a Cisco IP Phone using the configuration menus on the phone or using the phone's web page. For more information, see Chapter 5, "Configuring the Cisco IP Phone Models 7905G and 7912G Using the Phone Menus," and Chapter 7, "Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages."

For an explanation of profiles and how to use them, see Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server."

For instructions about accessing a phone's web page, see Chapter 7, "Configuring the Cisco IP Phone Models 7905G and 7912G Using Web Pages."

For a list of the configurable parameters on the phone menus and their equivalent profile and web page parameters, see Appendix B, "Phone Menu, Web Page, and Profile Equivalent Parameters."

This chapter includes the following sections:

- Network Parameters, page 8-2
- SIP Parameters, page 8-9
- Call Preference Parameters, page 8-13
- Tone Parameters, page 8-21
- Audio Parameters, page 8-24
- Profile Parameters, page 8-26
- DialPlan Parameter Detail, page 8-38
- Parameter Details, page 8-27

Network Parameters

Table 8-1describes the network parameters that you can configure through a phone's profile or through the Network Parameters area on the phone's web page.

Tip To access the Network Parameters area directly from a web browser, enter *ip_address*/**NetCfg**, where *ip_address* is the IP address of your Cisco IP Phone. This area appears by default when you enter *ip_address*/**dev**.

Table 8-1 Network Parameters

Parameter	Description
UseTftp	Enables or disables downloading of a profile from a TFTP server. If you set this parameter to 1 and subsequently make changes using the web interface, you must set this parameter to 0 before saving those changes; otherwise, the changes will be overwritten by the profile obtained from a TFTP server. • 0=Do not use a TFTP server. • 1=Use a TFTP server: – If TftpURL is set to 0, use the TFTP IP address or URL obtained from the DHCP server to contact the TFTP server. – If TftpURL is set to a value other than 0, use the specified IP address or URL to contact the TFTP server. **Note** Do not specify a port. The Cisco IP Phone always contacts the TFTP server at port 69. **Value type:** Boolean. **Default value:** 1
TftpURL	IP address or URL of the TFTP server from which a phone obtains a profile. Required if the DHCP server does not provide the TFTP server address. Optionally, you can include the path prefix to the profile to download. For example, if the TFTP server IP address is 192.168.2.170 or www.cisco.com, and the path to the file is /ip7905, you can specify the URL as 192.168.2.170/ip7905 or www.cisco.com/ip7905. Do not specify a port. The Cisco IP Phone always contacts the TFTP server at port 69. If DHCP is used, a nonzero values of TftpURL overwrites any DHCP-supplied addresses and values of 0 tell the phone to use DHCP-supplied addresses. This parameter is ignored if UseTftp is 0. **Value type:** IP address, up to 31 characters. **Default value:** 0.0.0.0

Table 8-1 Network Parameters (continued)

Parameter	Description
CfgInterval	Number of seconds between automatic profile refreshes from the TFTP server. At the earliest idle time following each interval expiration, the phone retrieves its profile using the **tftp get** command. Intervals should vary among phones on the network to prevent simultaneous contact of the TFTP server by many phones.This value can range from 60 to 4294967295. This parameter is ignored if UseTftp is 0. **Value type:** Integer. **Default value:** 3600
EncryptKey	Key for decrypting the configuration profile that is downloaded from the TFTP server. • 0=The configuration profile is not encrypted. • *string*=The profile is encrypted with this key. This parameter is ignored if UseTftp is 0. **Value type:** Alphanumeric string, up to 8 characters. **Default value:** 0
Dhcp	Specifies whether to use the DHCP server to obtain information such as IP addresses for the phone, the network gateway, and the DNS, NTP, and TFTP servers. If this parameter is 0, you must manually specify the IP address of the phone, and the IP addresses of the subnet mask and the default router used by the phone. See the "Minimum Configuration Settings for the Cisco IP Phone Models 7905G and 7912G" section on page 3-9 for more information. • 0=Do not use the DHCP server. Use hard-coded values. • 1=Use the DHCP server. **Value type:** Boolean. **Default value:** 1

Table 8-1 Network Parameters (continued)

Parameter	Description
StaticIP	Internet Protocol (IP) address of the phone. You can use this parameter to assign the IP address if DHCP does not provide it. If you assign an IP address with this parameter, you must also assign a default router and a subnet mask. See the StaticRoute and the StaticNetMask parameters in this table. This parameter is ignored if the Dchp parameter is set to 1. **Value type:** IP address. **Default value:** 0.0.0.0
StaticRoute	Static IP address of the network gateway. You can use this parameter to assign the IP address if DHCP does not provide it. This parameter is ignored if the Dchp parameter is set to 1. **Value type:** IP address. **Default value:** 0.0.0.0
StaticNetMask	Subnet mask used by the phone. You can use this parameter to assign the subnet mask if DHCP does not provide it. If you assign a Subnet Mask address with this parameter, you must also assign an IP address and a default router for the phone. See the StaticIP and the StaticRoute parameters in this table. This parameter is ignored if the Dchp parameter is set to 1. **Value type:** IP address. **Default value:** 0.0.0.0
Domain	Domain name of the phone. If set to 0, the phone will use the domain name supplied by the DHCP server. **Value type:** Alphanumeric string, up to 31 characters. **Default value:** 0

Table 8-1 Network Parameters (continued)

Parameter	Description
DNS1IP, DNS2IP	IP addresses of the primary and secondary domain name servers if DHCP is not used to provide the DNS addresses. If DHCP is used, nonzero values of DNS1IP and DNS2IP overwrite any DHCP-supplied addresses and values of 0 tell the phone to use DHCP-supplied addresses. Do not specify a port; the phone uses the default DNS port only. **Value type:** IP address. **Default value:** 0.0.0.0
NTPIP	IP address of the primary NTP server. DHCP may also supply a NTP server but NTPIP, if specified, overwrites that value. Do not specify a port; the phone uses the default NTP port only. If DHCP is used, a nonzero values of NTPIP overwrites any DHCP-supplied addresses and values of 0 tell the phone to use DHCP-supplied addresses. **Value type:** IP address. **Default value:** 0 (use DHCP)
AltNTPIP	IP address of a secondary NTP server if redundancy is desired. If only one NTP server exists, set this to 0 or to the address of the primary server. Do not specify a port; the phone uses the default NTP port only. **Value type:** IP address. **Default value:** 0 (use DHCP)
TimeZone	Offset to apply to the Greenwich Mean Time (GMT) returned by an NTP server to determine local time (to use for Call ID display, for example). Local time is generated as follows: • Local time = GMT + TimeZone, if TimeZone <= 12. • Local time = GMT + TimeZone – 25, if TimeZone > 12. For example, TimeZone = 17 for Pacific Standard Time. **Note** You must update this parameter manually when daylight savings time goes into effect and ends. **Value type:** Integer. **Default value:** 17

Table 8-1 Network Parameters (continued)

Parameter	Description
OpFlags	Enables or disables various operational features. • Bit 0: If 0, the TFTP phone-specific profile file name supplied by the DHCP server overwrites the default file name for each phone. If 1, the phone uses the default profile file phone-specific name (recommended). • Bit 1: If 0, enables probing of the static network router when the phone powers up. If 1, probing is disabled (recommended). • Bit 2: Reserved. • Bit 3: If 0, request DHCP option 150 in the DHCP discovery message. If 1, do not request this option. (Some DHCP servers do not respond if option 150 is requested.) • Bit 4: If 0, do not use VLAN ID set with the VLANSetting parameter. If 1, use VLAN ID (recommended). • Bit 5: If 0, use VLAN IP encapsulation. If 1, do not use VLAN IP encapsulation. • Bit 6: If 0, perform CDP discovery. If 1, do not perform CDP discovery. • Bit 7: If 0, allow configuration of the phone through the web. If 1, do not allow configuration through the web. • Bit 8: If 0, allow refreshing the phone through the web. If 1, do not allow refreshing the phone through the web. • Bit 9: If 0, allow resetting the phone through the web. If 1, do not allow resetting the phone through the web. • Bits 10-31: Reserved. **Value type:** Bitmap. **Default value:** 0x00000002

Table 8-1 Network Parameters (continued)

Parameter	Description
VLANSetting	Controls the use of VLAN in the phone. • Bits 0-2: Specifies 802.1Q priority for Signaling IP packets. • Bits 3-5: Specifies 802.1Q priority for Audio Voice IP packets. • Bits 6-17: Reserved. • Bits 18-29: User-specified 802.1Q VLAND ID. • Bits 30-31: Reserved. **Value type:** Bitmap. **Default value:** 0x0000002B
TOS	ToS (Type of Service) bits. Specifies the precedence and delay of Audio and Signaling IP packets. Higher values increase routing priority for data packets, resulting in less latency. • Bits 0-7: ToS value for audio data packets. Range: 0-255; Default: 184 • Bits 8-15: ToS value for signaling data packets. Range: 0-255; Default: 104 • Bits 16-31: Reserved **Value type:** Bitmap. **Default value:**0x000068b8

Table 8-1 Network Parameters (continued)

Parameter	Description
NPrintf	IP address and port of a host PC to which phone debug messages are sent, in the format *IP_address*.*port* (for example: 192.168.2.159.9000). **Note** The host PC must be running the prserv.exe application at the corresponding port. This application is available at Cisco.com. To turn off debugging, set to 0 or to 0.0.0.0.0. **Value type:** Extended IP address. **Default value:** 0.0.0.0.0 For more information about using Nprintf and prserv.exe to collect information for debugging, see the "Debugging" section on page 9-5.
TraceFlags	Enables specific trace features when Nprintf is set to a valid host address and port. • 0=Disable debug messages. • 1=Enable debug messages. **Value type:** Bitmap. **Default value:** 0x00000000

SIP Parameters

Table 8-2 describes the SIP parameters that you can configure through a phone's profile or through the SIP Parameters area on the phone's web page

Tip To access the SIP Parameters area directly from a web browser, enter *IP_address*/**SIPConfiguration**, where *IP_address* is the IP address of your Cisco IP Phone.

Table 8-2 SIP Parameters

Parameter	Description
UID, PWD	User ID and password for registration and authentication. Authentication can be performed on the (UID, PWD) pair or on the (LoginID, PWD) pair depending on the UseLoginID flag. However, the phone identifies itself to the outside world with the UID only and can be reached only with the corresponding UID but not the LoginID. If UID is set to "." or to "0" (zero), the phone is disabled (does not register with the proxy server). **Value type:** Alphanumeric string. **Default value:** UID=123, PWD=0
Proxy	SIP proxy server. **Value type:** Alphanumeric string. **Default value:** 0
AltProxyTimeOut	Timeout, in seconds, for switching from backup proxy server to primary proxy server. The value can range from 0 to 4294967295. **Value type:** Integer. **Default value:** 0
UseLoginID	Specifies which value to use for authentication: • 0=Use UID for authentication. • 1=Use LoginID for authentication. **Value type:** Boolean. **Default value:** 0
LoginID	Alternate user name used for authentication. **Value type:** Alphanumeric string. **Default value:** 0

Table 8-2 SIP Parameters (continued)

Parameter	Description
SIPRegInterval	SIP registration interval, in seconds, between each registration renewal to the SIP proxy server. If set to 0, the phone uses the default value. The value can range from 0 to 86400. **Value type:** Integer. **Default value:** 3600
MAXRedirect	Maximum number of redirections the phone attempts to reach a callee. The value can range from 0 to 10. **Value type:** Integer. **Default value:** 5
SIPRegOn	Whether to enable SIP registration. This parameter is ignored if a SIP proxy server is not specified. If set to 1, the phone periodically registers to the SIP proxy server at an interval given by the SIPRegInterval parameter. Valid values are 0 or 1. **Value type:** Boolean. **Default value:** 0
NATIP	Network Address Translation (NAT) WAN IP address where other SIP user agents can communicate with the phone. **Value type:** IP address. **Default value:** 0.0.0.0
SIPPort	Port where the phone listens for incoming requests and sends outgoing requests. Valid values are 5060 to 65535. **Value type:** Integer. **Default value:** 5060

Table 8-2 SIP Parameters (continued)

Parameter	Description
MediaPort	Port from which the phone transmits and receives media streams. This value must be an even number; each connection uses the next available even-numbered port for RTP. 0=Use the default value. This value can range from 0 to 65535. **Value type:** Even integer. **Default value:** 16384
OutBoundProxy	IP address or URL of the outbound proxy server, with or without a port parameter; for example, 209.165.201.30, 209.165.201.30.5060, 209.165.201.30:5061, sip.cisco.com, sip.xyz.cisco.com:5061. • For IP address, the port, if included, can be preceded by a period (.) or a colon (:). • For URL, the port must be preceded by a colon (:). • If no port is specified, the default port 5060 is used. **Value type:** Alphanumeric string, up to 31 characters. **Default value:** 0
NatServer	Specifies a server to which a dummy, single-byte UDP packed is sent to maintain a Network Address Translation (NAT) during a session. This parameter can contain up to 47 characters in fully qualified domain name (FQDN) or IP format with an optional port parameter (separated from the address by a colon); for example, xyz.cisco.com;1234. If no port is specified, the phone uses port 5060. **Value type:** IP address, up to 47 characters. **Default value:** 0.0.0.0 (port 5060 will be used)
NatTimer	Retransmission interval (in seconds) for sending a dummy packet to the server specified with the NatServer parameter, specified in bits 0-11 the parameter. The upper 20 bits are reserved and should be set to 0. **Value type:** Bitmap. **Default value:** 0x00000000 (no dummy packets will be sent to NatServer)

Table 8-2 SIP Parameters (continued)

Parameter	Description
DialPlan	Dial plan rules. No syntax check is performed by the implementation. The administrator must ensure that the dial plan is syntactically valid. See the "DialPlan Parameter Detail" section on page 8-38 for syntax and usage details. **Value type:** Alphanumeric string, up to 199 characters. **Default value:** *St4-|#St4-|911|1>#t8.r9t2-|0>#t811.rat4-|^1t4>#.-
IPDialPlan	Allows for detection of IP-like destination addresses in the dial plan: • 1=If two periods (.) are detected, assume that this is an IP address. • 2=If three periods (.) are detected, assume that this is an IP address. **Value type:** Integer. **Default value:** 1

Call Preference Parameters

Table 8-4 describes the call preference parameters that you can configure through a phone's profile or through the Call Preferences area on the phone's web page. These parameters specify various user features on the phone, and specifies which parameters appear and which options can be configured on a phone's Call Preference menu.

Tip To access the Call Preferences area directly from a web browser, enter *IP_address*/**CallPrefConfiguration**, where *IP_address* is the IP address of your Cisco IP Phone.

Table 8-3 Call Preference Parameters

Parameter	Description
Allow Call Waiting (on web page) CallWaiting (in profile)	Whether the call waiting feature is enabled on a phone. • 0=Disable the call waiting feature. • 1=Enable the call waiting feature. **Value type:** Boolean. **Default value:** 1
Allow Call Transfer (on web page) AttendedTransfer (in profile)	Whether the call transfer feature is enabled on a phone. If this feature is enabled, the **Trnsfer** softkey will appear when appropriate, allowing a user to transfer a call. If this feature is disabled, this softkey will never be available. • 0=Disable the call transfer feature. • 1=Enable the call transfer feature. **Value type:** Boolean. **Default value:** 1
Allow Blind Transfer (on web page) BlindTransfer (in profile)	Whether the blind call transfer feature is enabled on a phone. If this feature is enabled, the **BlndXfr** softkey will appear when appropriate, allowing a blind transfer of a call. If this feature is disabled, this softkey will never be available. • 0=Disable the blind call transfer feature. • 1=Enable the blind call transfer feature. **Value type:** Boolean. **Default value:** 1
Allow Conference (on web page) Conference (in profile)	Whether the conference feature is enabled on a phone. If this feature is enabled, the **Confrn** softkey will appear when appropriate, allowing a three-way conference to be established. If this feature is disabled, this softkey will never be available. • 0=Disable the conference feature. • 1=Enable the conference feature. **Value type:** Boolean. **Default value:** 1

Table 8-3 Call Preference Parameters (continued)

Parameter	Description
Block Caller ID (on web page) BlockCallerId (in profile)	Whether a phone's caller ID information, which includes the value specified by the Display Name parameter and the phone number, is sent with an outgoing call. If this parameter is enabled, outgoing calls will use "Anonymous" as the phone's caller ID. • 0=Do not block outgoing caller ID information. • 1=Block outgoing caller ID information. **Value type:** Boolean. **Default value:** 0
Block Anonymous Calls (on web page) BlockAnonymous (in profile)	Whether a phone rejects (blocks) an incoming call with "Anonymous" caller ID will be rejected. • 0=Do not block anonymous incoming calls. • 1=Block anonymous incoming calls. **Value type:** Boolean. **Default value:** 0
Do Not Disturb (on web page) DoNotDisturb (in profile)	Whether the Do Not Disturb feature is enabled on a phone. If this feature is enabled, calls to the phone will receive a busy signal. • 0=Disable the do not disturb feature. • 1=Enable the do not disturb feature. **Value type:** Boolean. **Default value:** 0
Voice Mail Number (on web page) VoiceMailNumber (in profile)	Specifies a telephone number where voice messages are stored and retrieved. If a number (other than 0) is specified: • The **Message** softkey will appear on the phone when appropriate. • Incoming calls forward to this number if the phone is busy or if the calls are not answered within the number of seconds specified with the Forward to VMail Delay(s) parameter. **Value type:** Alphanumeric string, up to 31 characters. **Default value:** 0 (disables this feature)

Table 8-3 Call Preference Parameters (continued)

Parameter	Description
Call Forward Number (on web page) CallForwardNumber (in profile)	Specifies a telephone number to which all calls to the phone are forwarded. If a number (other than 0) is specified, the Call Forward All feature is activated. **Value type:** Alphanumeric string, up to 31 characters. **Default value:** 0 (disables call forwarding)
Display Name (on web page) DisplayName (in profile)	Specifies a name to be used as part of the phone's caller ID and that will be displayed on the phone's LCD screen. A 0 (zero) or a blank value disables this feature. **Note** If the Block Caller ID parameter is set to Yes, outgoing calls will use "Anonymous" as the phone's caller ID regardless of the Display Name setting. **Value type:** Alphanumeric string, up to 31 characters. **Default value:** blank (no character string)
Short Name (on web page) ShortName (in profile)	Specifies a name to be displayed on the phone's LCD screen in place of the Display Name value. Short Name will not affect the Display Name value that is used as part of the phone's caller ID. **Value type:** Alphanumeric string, up to 31 characters. **Default value:** 0 (causes the Display Name value to be displayed)

Table 8-3 Call Preference Parameters (continued)

Parameter	Description
Time Format (on web page) TimeFormat (in profile)	Specifies the format for the time that appears on the phone's LCD screen. This format is specified by one or more of the following characters: h—designates the hour in 12-hour format. H—designates the hour in 24-hour format. i or I—designates minutes. a or A—for 12-hour format, include "p" with times from noon until one minute before midnight. : (colon)—displays a colon that blinks every second. For example, when the current time is 1:30 P.M., • h:ia causes the time to appear as 1:30 p. • H:I causes the time to appear as 13:30. **Value type:** Alphanumeric string, up to 15 characters. **Default value:** h:ia
Date Format (on web page) DateFormat (in profile)	Specifies the format for the date that appears on the phone's LCD screen. This format is specified by one or more of the following characters: m—designates the month as a number 1 through 12. M—designates the month as a three-letter abbreviation, Jan through Dec. d or D—designates the day of the month. y—designates a two-digit year (such as 03 for 2003). Y—designates a four-digit year. Other characters—appear as entered. For example, when the current date is March 10, 2003: • m-d-y causes the date to appear as 3-10-03. • M d, Y causes the date to appear as Mar 20, 2003. • Y/m/d causes the date to appear as 2003/3/10. **Value type:** Alphanumeric string, up to 15 characters. **Default value:** m-d-y

Table 8-3 Call Preference Parameters (continued)

Parameter	Description
Forward to VMail Delay (on web page) ForwardToVMDelay (in profile)	Specifies number of seconds after which an incoming call ringing at the phone will be forwarded to the telephone number specified by the Voice Mail Number parameter. Valid values are from 0 to 2147483647. **Value type:** Integer. **Default value:** 20 (seconds)

Table 8-3 Call Preference Parameters (continued)

Parameter	Description
GUI Show Mask (on web page) CallPrefGuiShow (in profile)	Specifies which parameters, if any, appear on the Call Preferences menu on the phone. Set a bit to 0 if the corresponding parameter should not appear. Set the bit to 1 if the parameter should appear. • Bit 0: Do Not Disturb. • Bit 1: Allow Call Waiting. • Bit 2: Block Caller ID. • Bit 3: Call Forward Number. • Bits 4–5: Reserved. • Bit 6: Display Name. • Bit 7: Time Format. • Bit 8: Date Format. • Bit 9: Voice Mail Number. • Bit 10: Allow Call Transfer. • Bit 11: Allow Attended Transfer. • Bit 12: Allow Conference. • Bit 13: Short Name. • Bits 14–23: Reserved. • Bit 24: Block Anonymous Call. • Bit 25: Reserved. • Bit 26: Forward to Voice Mail Delay. • Bit 27 and bits 29–31: Reserved. In addition, bit 28, if set to 1, causes a registration status icon to appear on the phone's LCD screen. This icon indicates whether the phone is registered to the SIP proxy server. **Value type:** Bitmap. **Default value:** 0xFFFFFFFF

Table 8-3 Call Preference Parameters (continued)

Parameter	Description
GUI Set Mask (on web page) CallPrefGuiSet (in profile)	Specifies which parameters on the Call Preferences menu on the phone can be changed by an end user. Set a bit to 0 if an end user should not be able to change the corresponding parameter. Set the bit to 1 if an end user should be able to change the parameter. • Bit 0: Do Not Disturb. • Bit 1: Allow Call Waiting. • Bit 2: Block Caller ID. • Bit 3: Call Forward Number. • Bits 4–5: Reserved. • Bit 6: Display Name. • Bit 7: Time Format. • Bit 8: Date Format. • Bit 9: Voice Mail Number. • Bit 10: Allow Call Transfer. • Bit 11: Allow Blind Transfer. • Bit 12: Allow Conference. • Bit 13: Short Name. • Bit 24: Block Anonymous Call. • Bit 25: Reserved. • Bit 26: Forward to Voice Mail Delay. **Value type:** Bitmap. **Default value:** 0xFFFFFFFFparameters:network<$startrange>

Tone Parameters

Table 8-4 describes the tone parameters that you can configure through a phone's profile or through the Tone Parameters area on the phone's web page. These parameters specify various tone characteristics for the Cisco IP Phone.

Tip To access the Tone Parameters area directly from a web browser, enter *IP_address*/**ToneConfiguration**, where *IP_address* is the IP address of your Cisco IP Phone.

Table 8-4 Tone Parameters

Parameter	Description
SigTimer	Timeout values for signal events. • Bits 0–7: CWT Period, which the number of 0.1-second intervals to wait between each burst of call-waiting tone. The range is 0 to 255. The default value is 100 (0x64, 10 seconds). 0=Use default. • Bits 8–13: Reserved. • Bits 14–19: Ring Timeout, which is the number of 10-second intervals to wait between when the phone starts ringing and the phone rejects the incoming call. Range: 0 to 63. 0=Never time out. Default value: 6 (0x6, 60 seconds). • Bits 20–25: NoAns Timeout, which is the number of seconds to wait between when the phone starts ringing and the phone initiates call forwarding on no answer. Range: 0 to 63. Default value: 20 (0x14, 20 seconds). • Bits 28–29: First Key Repeat Interval, which specifies how long a user must hold the **Volume** or the **Navigation** button up or down before the desired change begins to repeat. Valid values: 0 (1 second), 1 (disable repeat), 2 (2 seconds), and 3 (3 seconds). Default value: 0 (1 second). • Bits 30–31: Subsequent Key Repeat Interval, which specifies the intervals at which a change continues to repeat (after the First Key Repeat Interval) when a user continues to hold the **Volume** or the **Navigation** button up or down. Valid values: 0 (0.25 second), 1 (0.5 second), 2 (0.75 second), and 3 (1 second). Default value: 0 (0.25 second). **Value type:** Bitmap. **Default value:** 0x01418064

Table 8-4 Tone Parameters (continued)

Parameter	Description
RingOnOffTime	Specifies the ringer cadence pattern, expressed as three comma-separated integers *a*,*b*,*c*, where: • *a*—Number of seconds to wait before turning the ring on. • *b*—Number of seconds to wait before turning the ring off. • *c*—Ring frequency. **Value type:** Three comma-separated integers. **Default value:** 2,4,25
DialTone	Tone that plays when the phone is ready to accept the first digit of a telephone number or an IP address. See the "BusyTone, CallWaitTone, DialTone, DialTone2, and RingBackTone Parameter Details" section on page 8-28 for syntax and usage details. **Value type:** Array of 11 short integers. **Default value:** 2,31538,814,30831,2032,0,0,0,0,0,0
DialTone2	Secondary dial tone. For example, this tone might play after you dial a number to obtain an outside line. See the "BusyTone, CallWaitTone, DialTone, DialTone2, and RingBackTone Parameter Details" section on page 8-28 for syntax and usage details. **Value type:** Array of 11 short integers. **Default value:** 2,30743,1384,29864,1252,0,0,0,0,0,0
BusyTone	Tone that plays when the called party's line is busy. See the "BusyTone, CallWaitTone, DialTone, DialTone2, and RingBackTone Parameter Details" section on page 8-28 for syntax and usage details. **Value type:** Array of 11 short integers. **Default value:** 2,30467,1104,28959,1404,1,4000,4000,0,0,0

Table 8-4 Tone Parameters (continued)

Parameter	Description
ReorderTone	Tone that plays when the called number does not exist or when the external network circuit is busy. See the "ReorderTone Parameter Details" section on page 8-30 for syntax and usage details. **Value type:** Array of 17 short integers. **Default value:** 0,2,30467,1104,28959,1404,0,0,1,2000,2000,0,0,0,0,0,0
RingBackTone	Tone that plays when the called party's line is ringing. See the "BusyTone, CallWaitTone, DialTone, DialTone2, and RingBackTone Parameter Details" section on page 8-28 for syntax and usage details. **Value type:** Array of 11 short integers. **Default value:** 2,30831,2032,30467,1104,1,16000,32000,0,0,0
CallWaitTone	Tone that plays to indicate that you have a call waiting. See the "BusyTone, CallWaitTone, DialTone, DialTone2, and RingBackTone Parameter Details" section on page 8-28 for syntax and usage details. **Value type:** Array of 11 short integers. **Default value:** 1,30831,2412,0,0,1,2400,2400,0,0,4800

Audio Parameters

Table 8-5 describes the audio parameters that you can configure through a phone's profile or through the Audio Parameters area on the phone's web page. These parameters that specify encoding and other audio characteristics for the Cisco IP Phone.

Tip To access the Audio Parameters area directly from the a browser, enter *IP_address*/**AudioConfiguration**, where *IP_address* is the IP address of your Cisco IP Phone.

Table 8-5 Audio Parameters

Parameter	Description
RxCodec	Preferred audio decoder (receiving codec): • 1: G.711A-law • 2: G.711u-law • 3: G.729a **Value type:** Integer. **Default value:** 2
TxCodec	Preferred audio encoder (transmitting codec): • 1=G.711A-law • 2=G.711u-law • 3=G.729a **Value type:** Integer. **Default value:** 2
AudioMode	Audio operating mode. • Bit 0: G.711 silence suppression: – 0=Disable. – 1=Enable. • Bits 1–3: Reserved. • Bits 4–5: DTMF transmission method: – 0=Always inband. – 1=Negotiated via SDP. – 2=Always out-of-band. • Bits 6–31: Reserved. **Value type:** Bitmap. **Default value:** 0x00000011

Table 8-5 Audio Parameters (continued)

Parameter	Description
ConnectMode	Connection mode for the selected call-signaling protocol. See the "ConnectMode Detail" section on page 8-36 for syntax and usage details. **Value type:** Bitmap. **Default value:** 0x00000000
NumTxFrames	Number of frames per outbound audio RTP packet. For G.711 and G.729 codecs, a frame is 10 ms. Cisco recommends that you use the default value. Valid values are 1, 2, 3, 4, 5, or 6. **Value type:** Integer. **Default value:** 2

Profile Parameters

Table 8-6 describes the parameters that you can configure through a phone's profile only.

For more information about profiles, see Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server."

Table 8-6 Profile Parameters

Parameter	Description
UIPassword	Password to access the phone's configuration web page, and to unlock the phone's Network Configuration and SIP Configuration menus for editing. If set to 0, configuration parameters cannot be modified from a phone's web page. In addition, if set to 0, the phone will not prompt for a password when you unlock configuration parameters on the phone. **Value type:** Alphanumeric string up to nine characters.
upgradecode	Provides information for upgrading the firmware image on the phone. See the "Upgradecode Parameter Detail" section on page 8-41 for syntax and usage details.

Table 8-6 Profile Parameters (continued)

Parameter	Description
upgradelogo	Allows you to specify the graphic that appears on the phone's LCD screen. See the "Upgradelogo Parameter Detail" section on page 8-43 for syntax and usage details.
Include	Includes the parameters and values from another profile when you create the binary profile. Specify the file to include as an alphanumeric string. For example, if you are creating a phone-specific profile and want to include some values from a common profile, called common.txt, put this parameter and value in the text phone-specific profile: `include:common.txt` When you run the cfgfmt.exe to create the binary profile from the text profile, the parameters and values from common.txt will be included in the binary profile. Cisco recommends that the Include parameter, if used, be the first parameter in a text profile file. Any parameters in a text profile that come before an include statement will be overwritten with values from the same parameters, if they exist, in a common profile.

Parameter Details

This section includes details about using the following parameters:

- BusyTone, CallWaitTone, DialTone, DialTone2, and RingBackTone Parameter Details, page 8-28
- ReorderTone Parameter Details, page 8-30
- ConnectMode Detail, page 8-36
- DialPlan Parameter Detail, page 8-38
- Upgradecode Parameter Detail, page 8-41
- Upgradelogo Parameter Detail, page 8-43

BusyTone, CallWaitTone, DialTone, DialTone2, and RingBackTone Parameter Details

The following parameters specify tones that can consist of a single frequency or of two frequencies that play simultaneously, and of a cadence with up to two on-off pairs:

- BusyTone—Tone that plays when the called party's line is busy
- CallWaitTone—Tone that plays to indicate that you have a call waiting
- DialTone—Tone that plays when the phone is ready to accept the first digit of a telephone number or an IP address
- DialTone2—Secondary dial tone (for example, the dial tone that plays when you dial a number to obtain an outside line)
- RingBackTone—Tone that plays to indicate that the called party's line is ringing

For the default values of these parameters, which are suitable for the United Sates, see Table 8-4.

The syntax of these parameters is:

parameter:*NumOfFreqs*,*TFreq_1*,*TAmplitude_1*,*TFreq_2*,*TAmplitude_2*,
NumOfOnOffPairs,*OnTime_1*,*OffTime_1*,*OnTime_2*,*OffTime_2*,*TotalToneTime*

where:

- *parameter* is BusyTone, CallWaitTone, DialTone, DialTone2, or RingBackTone.
- *NumOfFreqs* is the number of frequencies in the tone (1 or 2).
- *TFreq_1* and *TFreq_2* are the transformed frequencies of the first and second frequencies, respectively. Calculate each value as follows, where *Frequency* is the desired frequency in Hz:

  32767 * cos(2 * pi * *Frequency*/8000)

  The range of each value is –32768 to 32767.

  Set a value to 0 if the frequency does not exist.

  For negative values, use the 16-bit 2's complement value. For example, enter –1 as 65535 or as 0xffff.

- *TAmplitude_1* and *TAmplitude_2* are the transformed amplitudes (volumes) of the first and second frequencies, respectively. Calculate each value as follows:

  A * 32767 * sin(2 * pi * *Frequency*/8000)

  where:

  – *A* is the amplitude factor, which controls the volume. This value is calculated as follows, where *k* is the desired volume in dBm and *n* is the number of frequencies (1 or 2):

  $A = 0.5 * 10^{((k + 9 - (n - 1) * 3) / 20)}$

  For example, for a one-frequency tone with a volume of –19 dBm,

  $A = 0.5 * 10^{((-19 + 9)/20)} = 0.16$

  – *Frequency* is the desired frequency in Hz

- *NumOfOnOffPairs* is the number of on-off pairs in the cadence of the tone (0, 1, or 2). For a steady tone, use 0.

  If this value is 0, the *OnTime_1*, *OnTime_2*, *OffTime_1*, and *OffTime_2* values must also be 0.

- *OnTime_1* and *OnTime_2* are the lengths of time that the first and second on-off pairs of a cadence play a sound, respectively. (See Figure 8-1 for a graphical representation.)

  Specify each value as a number of samples with the sampling rate of 8 kHz. The range of each value is 0 to 0xffff.

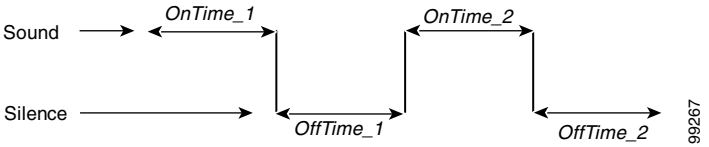
  For example, for a length of 0.3 seconds, set a value to 2400.

- *OffTime_1* and *OffTime_2* are the lengths of silence after the sound of the first and second on-off pairs of a cadence, respectively. (See Figure 8-1 for a graphical representation.)

  Specify each value as a number of samples with the sampling rate of 8 kHz. The range of each value is 0 to 0xffff.

  For example, for a length of 0.3 seconds, set a value to 2400.

Figure 8-1 Cadence with Two On-Off Pairs



- *TotalToneTime* is the total length of time that the tone plays. If this value is 0, the tone will play until another call event stops the tone.

  For the BusyTone, DialTone, DialTone 2, and RingBackTone parameters, specify this value in 10 ms units (100 ms = 1 second). For the CallWaitTone parameter, specify this value as a number of samples with the sampling rate of 8 kHz.

ReorderTone Parameter Details

The ReorderTone parameter specifies the tone that plays when the called number is not available or the external circuit is busy. This tone can consist of either

- Up to three frequencies played simultaneously and a cadence of up to three on-off pairs. The first on-off pair can repeat multiple times before the second on-off pair plays.

  For example, a 400 Hz frequency plays four times for 0.75 second followed by 0.1 second of silence after each play and then plays one time for 0.75 second followed by 0.4 second of silence. This pattern can be set to repeat until another call event stops it.

- Up to three frequencies played sequentially with a cadence of up to three on-off pairs

  For example, the frequencies 900 Hz, 1400 Hz, and 1800 Hz play sequentially for 0.33 seconds each with no silence after the first and second frequencies but 1 second of silence after the third frequency.

For the default value of this parameter, which is suitable for the United States, see Table 8-4.

The syntax of the ReorderTone parameters is:

`ReorderTone:`*`Sequential`*`,`*`NumOfFreq`*`s,`*`TFreq_1`*`,`*`TAmplitude_1`*`,`*`TFreq_2`*`,`
`TAmplitude_2``,TFreq_3,`*`TAmplitude_3`*`,`*`NumOfOnOffPairs`*`,`*`OnTime_1`*`,`*`OffTime_1`*`,`
`OnTime_2``,`*`OffTime_2`*`,`*`OnTime_3`*`,`*`OffTime_3`*`,`*`NumOfRepeats`*`,`*`TotalToneTime`*

where:

- *Sequential* specifies whether multiple frequencies in a tone play simultaneously (0) or sequentially (1). Set to 0 for a tone with one frequency.
- *NumOfFreqs* is the number of frequencies in the tone (1, 2, or 3). The frequencies can play simultaneously or sequentially, depending on the *Sequential* setting.
- *TFreq_1*, *TFreq_2*, and *TFreq_3* are the transformed frequencies of the first, second, and third frequencies, respectively. Calculate each value as follows, where *Frequency* is the desired frequency in Hz:

  32767 * cos(2 * pi * *Frequency*/8000)

  The range of each value is –32768 to 32767.

  Set a value to 0 if the frequency does not exist.

  For negative values, use the 16-bit 2's complement value. For example, enter –1 as 65535 or as 0xffff.

- *TAmplitude_1*, *TAmplitude_2*, and *TAmplitude_3* are the transformed amplitudes (volumes) of the first, second, and third frequencies, respectively. Calculate each value as follows:

  A * 32767 * sin(2 * pi * *Frequency*/8000)

  where:

  – *A* is the amplitude factor, which controls the volume. Calculate this value as follows, where *k* is the desired volume in dBm and *n* is the number of frequencies (1, 2, or 3):

    $A = 0.5 * 10^{((k + 9 - (n - 1) * 3) / 20)}$

    For example, for a one-frequency tone with a volume of –19 dBm,

    $A = 0.5 * 10^{((-19 + 9)/20)} = 0.16$

  – *Frequency* is the desired frequency in Hz

- *NumOfOnOffPairs* is the number of on-off pairs in the cadences of the tone (0, 1, 2, or 3). For a steady tone, use 0.

  If this value is 0, the *OnTime_1*, *OnTime_2*, *OnTime_ 3*, *OffTime_1*, *OffTime_2*, and *OffTime_3* values must also be 0.

- *OnTime_1*, *OnTime_2*, and *OnTime_3* are the lengths of time that the first, second, and third on-off pairs of a cadence play a sound, respectively. (See Figure 8-2 for a graphical representation.)

  Specify each value as a number of samples with the sampling rate of 8 kHz. The range of each value is 0 to 0xffff.

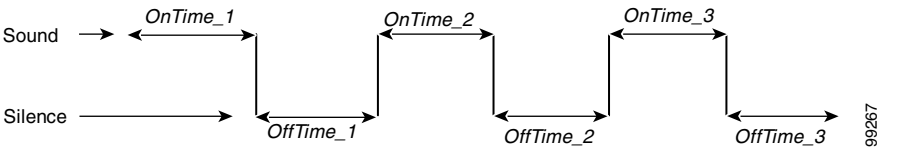
  For example, for a length of 0.3 seconds, set a value to 2400.

- *OffTime_1*, *OffTime_2*, and *OffTime_3* are the lengths of silence after the sound of the first, second, and third on-off pairs of a cadence, respectively.

  Specify each value as a number of samples with the sampling rate of 8 kHz. The range of each value is 0 to 0xffff.

  For example, for a length of 0.3 seconds, set a value to 2400. (See Figure 8-2 for a graphical representation.)

Figure 8-2 Cadence with Three On-Off Pairs



- *NumOfRepeats* is the number of times that the first on-off pair of the cadence (specified by *OnTime_1*, *OffTime_1*) repeats before the second on-off pair (specified by *OnTime_2*, *OffTime_2*) plays.

  For example, if *NumOfRepeats* is 2, the first on-off pair will play three times (it will play once and then repeat two times), then the second on-off pair will play.

- *TotalToneTime* is the total length of time that the tone plays. If this value is 0, the tone will play until another call event stops the tone.

  This value is in 10 ms units (100 ms = 1 second).

ReorderTone Parameter Example1

Assume that you want a reorder tone in which:

- The frequencies 900 Hz, 1400 Hz, and 1800 Hz play sequentially.
- Each frequency plays once for 0.33 seconds.
- There is no silence after the first and the second frequencies.
- There is 1 second of silence after the third frequency (before the first frequency starts again)
- The volume of each frequency is –19 dBm.
- The tone plays until another call event stops the tone.

For this reorder tone, make the following setting. See Table 8-7 for a detailed explanation.

```
ReorderTone:1,3,24917,3405,14876,4671,5126,5178,3,2640,0,2640,0,
2640,8000,0,0
```

Table 8-7 Reorder Tone Parameter Example 1 Explanation

Component	Setting	Explanation
Sequential	1	Frequencies play sequentially
NumOfFreqs	3	Three frequencies in the tone
TFreq_1	24917	First frequency is 900 Hz
TAmplitude_1	3405	First frequency volume is –19 dBm
TFreq_2	14876	Second frequency is 1400 Hz
TAmplitude_2	4671	Second frequency volume is –19 dBm
TFreq_3	5126	Third frequency is 1800 Hz
TAmplitude_3	5178	Third frequency volume is –19 dBm
NumOfOnOffPairs	3	Three on-off pairs in the cadence of the tone
OnTime_1	2640	Sound in first on-off pair plays for 0.33 seconds
OffTime_1	0	No silence after the first sound (the second sound plays immediately)
OnTime_2	2640	Sound in second on-off pair plays for 0.33 seconds

Table 8-7 Reorder Tone Parameter Example 1 Explanation (continued)

Component	Setting	Explanation
OffTime_2	0	No silence after the second sound (the third sound plays immediately)
OnTime_3	2640	Sound in third on-off pair plays for 0.33 seconds
OffTime_3	8000	1 second of silence after the sound in the third on-off pair (before the pattern repeats, beginning with the first on-off pair)
NumOfRepeats	0	First on-off pair of the cadence plays once (does not repeat), then the second on-off pair plays
TotalToneTime	0	Tone plays continuously (set of three on-off pairs of the cadence repeat continuously) until another call event stops the tone

ReorderTone Parameter Example 2

Assume that you want a reorder tone in which:

- The only frequency is 400 Hz.
- The frequency plays six times, each time for 0.1 second followed by 0.9 second of silence.
- The frequency then plays once for 0.3 second followed by 0.7 second of silence.
- The volume of the frequency is –19 dBm.
- The tone plays until another call event stops the tone.

For this reorder tone, make the following setting. See Table 8-8 for a detailed explanation.

```
ReorderTone:0,1,31164,1620,0,0,0,0,2,800,7200,2400,5600,0,0,5,0
```

Table 8-8 Reorder Tone Parameter Example 2 Explanation

Component	Setting	Explanation
Sequential	0	Required setting for a tone with one frequency
NumOfFreqs	1	One frequency in the tone
TFreq_1	31164	First frequency is 400 Hz
TAmplitude_1	1620	First frequency volume is –19 dBm
TFreq_2	0	No second frequency
TAmplitude_2	0	No second frequency
TFreq_3	0	No third frequency
TAmplitude_3	0	No third frequency
NumOfOnOffPairs	2	Two on-off pairs in the cadence of the tone
OnTime_1	800	Sound in first on-off pair plays for 0.1 second
OffTime_1	7200	Sound in first on-off pair is followed by 0.9 second of silence
OnTime_2	2400	Sound in second on-off pair plays for 0.3 seconds
OffTime_2	5600	Sound in second on-off pair is followed by 0.7 second of silence
OnTime_3	0	No third on-off pair in the cadence
OffTime_3	0	No third on-off pair in the cadence
NumOfRepeats	5	First on-off pair of the cadence plays six times (plays once and then repeats five times), then the second on-off pair plays
TotalToneTime	0	Tone plays continuously (set of two on-off pairs of the cadence repeat continuously) until another call event stops the tone

ConnectMode Detail

The ConnectMode parameter specifies the connection mode for the selected call-signaling protocol, as described in Table 8-9.

Table 8-9 ConnectMode Parameter

Bit	Description
0–15	Reserved. Must be set to 0.
16	Registration removal prior to re-registration. • 0=Disable (default). • 1=When the phone powers up, “Contact: *” is used to remove all registrations. On subsequent registration cycles, “Contact: *current_SIP_URL*;expires=0” is used.
17–18	Reserved. Must be set to 0.
19	IP ringback and early media. • 0=Do not send a ringback tone to the caller (default). • 1=Send a ring back tone to the caller.
20	Include “action=proxy” in REGISTER request. Do not enable if bit 21 is enabled. • 0=Disable (default). • 1=Enable.
21	Include “action=redirect” in REGISTER request. • 0=Disable (default). • 1=Enable.

Table 8-9 ConnectMode Parameter (continued)

Bit	Description
22	Process a *received* = parameter in the VIA header to extract the external IP addresses used by the Network Address Translation (NAT) router. • 0=Disable (default). • 1=Enable. When a Cisco IP Phone is operating behind a NAT, the NATIP parameter must be set to the external IP address of the NAT router. This setting allows the correct IP address to be placed in the Contact and SDP headers. You may leave the NATIP address set to the default value of 0 (or 0.0.0.0) and let the phone automatically scan the VIA header for a *received* = parameter. The parameter, if present, would indicate that the phone is operating behind a firewall. The phone proceeds as follows: **1.** If the *received* = parameter is an INVITE response, the current INVITE is canceled and a new INVITE is sent with the new IP address extracted from the received =*NAT_IP_Address* parameter in the Contact header. This step is performed only if registration is currently in an idle state. **2.** If the *received* = parameter is in a REGISTER response as a result of a REGISTER command, the phone will cancel all previous registrations and re-register with the new IP address extracted from the received = *NAT_IP_Address* parameter in the Contact header. **Note** For the phone to automatically detect its presence behind a NAT, the SIP proxy server or remote user agent server must include the *received* = parameter in the VIA header in the responses to the phone if the proxy detects that the source address and port do not match those in the VIA header.
23	Reserved. Must be set to 0.

Table 8-9 ConnectMode Parameter (continued)

Bit	Description
24	Include RTP statistics in BYE request and response. • 0=Disable (default). • 1=Enable. If this bit is enabled, the phone will insert the headers RxStat and TxStat as follows: RxStat: *Dur=a,Pkt=b,Oct=c,LatePkt=d,LostPkt=e,AvgJit=f* TxStat: *Dur=g,Pkt=h,Oct=i* where: • *Dur* is the total number of seconds since the beginning of reception or transmission • *Pkt* is the total number of RTP packets received or transmitted • *Oct* is the total number of RTP payload octets received or transmitted (not including RTP header) • *LatePkt* is the total number of late RTP packets received • *LostPkt* is the total number of lost RTP packets received (not including late RTP packets) • *AvgJit* is the average jitter, which is an estimate of the statistical variance of the RTP packet inter-arrival time, measured in timestamp unit and calculated according to RFC 1889. • *a*, *b*, *c*, *d*, *e*, *f*, *g*, *h*, and *i* are integers
25–31	Reserved. Must be set to 0.

DialPlan Parameter Detail

The DialPlan parameter specifies dial plan rules.

Note No syntax check is performed by the implementation of this parameter. It is the responsibility of the provisioner to make sure that the dial plan is syntactically valid.

The DialPlan field provides programmable strings of dial plan that allow you to specify:

- Special rule—I*timeout* to control default interdigit timeout. Specifying this rule also has the side effect of preventing nonmatching dial strings from being sent out.
- Optional send character to use. For example, the pound sign (#) or the asterisk (*).
- Number of digits before auto-send.
- Send after timeout at any specified number of digits (timeout can be changed as digits are entered).

The DialPlan field uses the following conventions:

- Special characters translate as shown in Table 8-10.

Table 8-10 DialPlan Parameter Special Characters

Character	Action
Period (.)	Match any digit.
Comma (,)	Play secondary dial tone as specified by DialTone2.
Hyphen (-)	More digits can be entered. If this character is needed, it must appear at the end of an individual rule. For example, 1408t5- is legal, but 1408t5-3... is illegal.
Pound sign (#)	The terminating key to send is #, and termination can be applied only after matching hits >#. So >* means that the terminating character is the asterisk (*); that is, the terminating key must follow the greater-than sign (>).
Characters “t*n*”	Set the timeout to *n* seconds. Note: n is 0–9 and a–z, which ranges from 0 to 26.
Characters “r*n*”	Repeat the last pattern *n* times. Note: The characters “>#” and “tn” are modifiers, not patterns. n is 0–9 and a–z, which ranges from 0 to 26. Use the repeat modifier to specify more rules in less space.
Modifier “S”	Cause rule-matching to cease (that is, if a rule matches and the modifier “S” is seen, all other rules after that matching rule are not used for matching).

- Rules are applied in the listed order. The first rule that completely matches triggers the send.
- Multiple rules are separated by a pipe (|).

Dial Plan Rules Example 1

The following two sets of dial plan rules are translated as described in Table 8-11:

```
“.t7>#......t4-|911|1t7>#.........t1-|0t4>#.t7-”
```

```
“.t7>#r6t4-|911|1t7>#.r9t1-|0t4>#.t7-”
```

Table 8-11 Dial Plan Rules Example 1 Explanation

String	Effect
`.t7>#......t4-`	At least one digit needs to be entered. After that, send after 7 seconds. The terminating # character can also be applied after the first digit is entered. After 7 digits are entered, the timeout changes to 4 seconds. The * character means that more digits can be entered, as long as the string is not terminated by timeout or #.
`911`	Send immediately.
`1t7>#.........t1-`	At least one digit needs to be entered. After that, send after 7 seconds. The terminating character # can also be applied after the first digit is entered. After 10 digits are entered, the timeout changes to 1 second. The * character means that more digits can be entered, as long as the string is not terminated by timeout or #.
`0t4>#.t7-”`	After a 0, if no other digit is entered, send after 4 seconds. If another digit is entered, send after 7 seconds. Again, # is the terminating digit.

Dial Plan Rules Example 2

The following set of dial plan rules is translated as described in Table 8-12:

```
"911|1>#.r9t3.t5-|0t411t9-"
```

Table 8-12 Dial Plan Rules Example 2 Explanation

String	Effect
`911`	Send immediately.
`1>#.r9t3.t5-`	If 14088713344 is entered, send after 3 seconds. If another digit is entered (for example, 140887133445), send after 5 seconds.
`0t411t9-`	If 0 is entered, send after 4 seconds. If 011 is entered, send after 9 seconds.

Upgradecode Parameter Detail

The upgradecode parameter provides the phone with instructions it uses to download the latest firmware image from the TFTP server. (For information about editing a profile, see Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server.")

The syntax of the upgradecode parameter is:

`upgradecode:3,`*`type`*`,0x0400,0x0100,`*`tftp_server_ip`*`,69,`*`image_id`*`,`
`image_file_name`

where:

- *type* is 0x501 for the Cisco IP Phone 7905G or 0x601 for the Cisco IP Phone 7912G.
- *tftp_server_ip* is the IP address of the TFTP server on which the firmware upgrade image is stored. Enter 0 to use the TFTP server specified by the TFTPServer1 parameter or by DHCP.
- *image_id* is a unique 32-bit integer value. This value must be different for each upgrade. For this value, use 0x followed by the build date on the firmware image file name. (For example, if the image file name is CP79050101SIP030323A.ZUP, then the build date is 030323A, and *image_id* would be 0x030323A.)

- *image_file_name* is the file name of the firmware image, in the following format. (This format includes spaces between elements for clarity. Do not include spaces between elements when you enter and image file name in the upgradecode parameter.)

  `CP model VV vv RR SIP yymmdd a-f ext`

  where:

  – *model* is 7905 for the Cisco IP Phone 7905G or 7912 for the Cisco IP Phone 7912G

  – *VV* is the major version number (always two digits)

  – *vv* is the minor version number (always two digits)

  – *RR* is build revision number (always two digits)

  – SIP is the protocol and should not be changed

  – yymmdd is a two-digit year, two-digit month, and two-digit day

  – a-f is the build letter (*yymmdd* and a-f together form the build date of the image

  – *ext* is the extension .zup or .sbin

When you enter the upgradecode parameter, you must enter the following values exactly as shown in the syntax:

- **3** (preceding *type*)
- **0x0400, 0x0100** (preceding *tftp_server_ip*)
- **69** (default TFTP server port number, preceding *image_id*)

Note A firmware image can contain a signature that allows a phone to verify the authenticity of the image. A firmware image with such a signature has the extension .sbin. A firmware image without such a signature has the extension .zup. A Cisco IP Phone 7905G that cannot perform image authentication will request a .zup image, which will provide it with the ability to verify the authenticity of .sbin images in

future upgrades. A phone that can perform image authentication will only request a .sbin file. If the profile of a phone that can perform image authentication specifies a .zup firmware image instead of a .sbin firmware image, the phone will automatically modify the request to obtain a .sbin firmware image. (A Cisco IP Phone 7912G will always request a .sbin image.)

The default value for the upgradecode parameter is:

3,0x501,0x0400,0x0100,0.0.0.0,69,0,none

Use this default value as a starting point when you enter a value. (This default value includes 0x501 for a Cisco IP Phone 7905G. If you are using a Cisco IP Phone 7912G, make sure to change 0x501 to 0x601.)

Process

When you store a new firmware image on the TFTP server and you update *image_id* in the upgradecode parameter, the Cisco IP Phone upgrades its firmware with the new image. The phone contacts the TFTP server that is specified by *tftp_server_ip* in the upgradecode parameter.

Example

```
upgradecode:3,0x501,0x0400,0x0100,192.168.2.170,69,0x030609a,CP7905010
1SIP030609A.zup
```

This parameter setting instructs a Cisco IP Phone 7905G to upgrade its firmware to CP79050101SIP030609A.zup by downloading this file from the TFTP server IP address of 192.168.2.170. This download occurs after the phone downloads its configuration file that contains the upgradecode parameter and only if the phone's internally-cached image_id is different than the value 0x030609a.

Upgradelogo Parameter Detail

When the Cisco IP Phone is not in use for a call, a figure appears on the LCD screen above the soft key labels and below the time and date. Using TFTP configuration, you can change this figure to one that you provide. For example, you might change the figure to your company logo.

Before you can change the figure on the phone, you must use a graphics program to create an image with the following attributes:

- Width of 88 pixels.
- Height of 27 pixels.
- Monochrome (black-and-white).
- Saved as bitmap file with the extension .bmp. For example, mylogo.bmp.

In addition, you will need the bmp2logo.exe tool, which converts your bitmap image file to a .logo file that can be downloaded to the phone. This tool is bundled with the Cisco IP Phone software.

To change the figure that appears on a Cisco IP Phone, perform the following steps. As part of this procedure, you will need to update the phone's profile. For information about editing a profile, see Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server."

Procedure

Step 1 Open a command window and type the following command:

`bmp2logo` *`imageID image`*`.bmp` *`image`*`.logo`

where:

- *imageID* is a unique identifier for the new figure. This identifier must be a number from 0 through 4294967295 and must be different than the identifier of the figure that is currently on the phone.
- *image* is the base file name of the image that you previously created and saved with the graphics program.

Note The imageID of the image that comes with the phone is 1.

For example, if the image identifier is 10 and the base name of your image file is mylogo, type this command:

```
bmp2logo 10 mylogo.bmp mylogo.logo
```

Step 2 Copy the *image*.logo file to the root directory on the TFTP server.

Step 3 Add the following line to the Cisco IP Phone profile:

`upgradelogo:`*`imageID`*`,`*`TFTPServerIP`*`,`*`image`*`.logo`

where:

- *imageID* is the same unique identifier that you specified in Step 1.
- *TFTPServerIP* is the IP address of the TFTP server on which the *image*.logo file is stored. If the *image*.logo file is stored on the same TFTP server as the Cisco IP Phone configuration file, replace *TFTPServerIP* with the numeral 0.
- *image* is the base file name of the image file.

For example, if the image identifier is 10, the converted file is stored on the same TFTP server as the Cisco IP Phone configuration file, and the base name of the converted image file is mylogo, add the following line to the configuration file:

```
upgradelogo:10,0,mylogo.logo
```

Troubleshooting the Cisco IP Phone Models 7905G and 7912G

This chapter describes some basic testing and troubleshooting procedures for the Cisco IP Phone models 7905G and 7912G. It contains the following sections:

- General Troubleshooting Tips, page 9-1
- Resolving Problems, page 9-2
- Contacting TAC, page 9-5
- Debugging, page 9-5

General Troubleshooting Tips

The suggestions in this section are general troubleshooting tips.

- If using a Dynamic Host Configuration Protocol (DHCP) server, make sure that it is operating correctly. The DHCP server should show an incoming request from the MAC address listed on the product label.
- If you do not see the status screen after you connect the Ethernet cable, make sure the power cord and the Ethernet connection are secure.
- If you do not hear a dial tone, make sure that the telephone-handset line cord is plugged into the Cisco IP Phone port. Also make sure that the appropriate Ethernet cable (crossover or straight-through) is used, and that all cable connections are secure.

- A fast-busy tone indicates that the number you called is not valid or that external circuits are busy. Verify the number or try your call again later.
- If you place a call to another IP telephone, hear ringback, and the called party answers but you cannot hear the speaker's voice, verify that the Cisco IP Phone and the other IP telephone support at least one common audio codec (G.711 A-law, G.711 u-law, or G.729a).
- If you use a Cisco PIX firewall, make sure that it is version 5 or later.

Related Topics

- Resolving Problems, page 9-2
- Contacting TAC, page 9-5
- Debugging, page 9-5

Resolving Problems

This section describes errors or unexpected results that you may encounter with the Cisco IP Phone models 7905G and 7912G. It includes possible causes and recommended actions, where appropriate.

Symptom Parameters with values set through a phone's web interface or LCD screen revert to their original settings.

Possible Cause You are using TFTP for configuring the phone (the UseTFTP parameter is set to 1). Parameter values in a profile will overwrite values that you set from a phone's Network Configuration menu, its SIP Configuration menu, or its web page.

Recommended Action If you are using TFTP to configure phones, do not use the web page or the phone menus to modify SIP or network parameter values. Use the phone's Network Configuration menu only to initially configure phone.

Symptom Time is not displayed or is displayed incorrectly on the phone.

Possible Cause

- A Network Time Protocol (NTP) server is not specified for the phone or the NTP server is returning an incorrect time.
- The TimeZone parameter (in the profile or a phone's web page) or the Time Zone parameter (in the Network Configuration menu) is not set correctly.

Recommended Action

- Specify at least one NTP server for the phone and check the NTP server.
- Verify the setting of the TimeZone or the Time Zone parameter. (You must update the TimeZone or the Time Zone parameter value manually when daylight savings time goes into effect and ends.)

Symptom The phone plays a fast busy tone.

Possible Cause User name or password is incorrect.

Recommended Action Verify that the user name and password are correct.

Symptom Ready screen does not appear on the phone.

Possible Cause

- The Cisco IP Phone is trying to obtain the DHCP address or the firmware image is being upgraded.
- The Ethernet cable is unplugged.

Recommended Action

- Wait for a few moments.
- Plug in the Ethernet cable.

Symptom There is no dial tone on the phone.

Possible Cause No user ID was entered, or the UID parameter is set to 0 or a period (.).

Recommended Action Verify the UID parameter value and enter the correct user ID.

Symptom The phone plays an incorrect busy tone, call waiting tone, dial tone, reorder tone, or ringback tone.

Possible Cause There is an incorrect setting for the BusyTone, CallWaitTone, DialTone, DialTone2, RingBackTone, or ReorderTone parameter.

Recommended Action Verify that these parameters are set correctly for your country. For more information, see the "BusyTone, CallWaitTone, DialTone, DialTone2, and RingBackTone Parameter Details" section on page 8-28 or the "ReorderTone Parameter Details" section on page 8-30.

Symptom Cisco IP Phone 7905G resets repeatedly after upgrading its firmware image.

Possible Cause The phone cannot perform image authentication, but it has upgraded to a .SBIN firmware image file instead of to a .ZUP image file. (A .SBIN firmware image file requires that the phone be able to perform image authentication.)

Recommended Action Upgrade the phone to a .ZUP image file. For more information, see the "Upgradecode Parameter Detail" section on page 8-41.

Symptom The Cisco logo does not appear properly on the web page for a phone.

Possible Cause You are using Netscape version 4.78 or earlier.

Recommended Action When accessing a phones web page, use Netscape release 6.0 or later, or use Internet Explorer.

Related Topics

- General Troubleshooting Tips, page 9-1
- Contacting TAC, page 9-5
- Debugging, page 9-5

Contacting TAC

If you need to contact the Cisco Technical Assistance Center (TAC) as explained in the "Obtaining Technical Assistance" section on page xiv, be prepared to provide the following information:

- Product type.
- Software version number, hardware version number, and serial number. To identify these numbers from a phone, choose **Menu > Settings > Status > Firmware Versions**. You can also identify the MAC address from the Device Information area of the Cisco IP Phone web page.
- MAC address. To identify this information from a phone, choose **Menu > Settings > Network Configuration** and scroll to the MAC Address parameter. You can also identify the MAC address from the Device Information area of the Cisco IP Phone web page.

Debugging

You can collect information relating to the operations of a Cisco IP Phone and store this information in a log file on a server that you specify.This information can be useful for debugging and troubleshooting.

To collect information for debugging, you will need the prserv.exe tool. This tool is bundled with the Cisco IP Phone software.

To collect debugging information in a log file, perform the following steps. For information about editing the Cisco IP Phone profile, see Chapter 6, "Configuring the Cisco IP Phone Models 7905G and 7912G Using a TFTP Server."

Step 1 Add the following line to the Cisco IP Phone profile:

`Nprintf:`*`IPaddress.listen_port`*

where:

- *IPaddress* is the IP address of the server to which information will be sent.
- *listen_port* is the port to which information is sent on the server specified.

For example, if you want to send information to port 9001 on a server with an IP address of 192.168.2.170, set the Nprintf parameter to 192.168.2.170.9001.

Note If you set this parameter to 0 or to 0.0.0.0, no information will be sent from the phone.

Step 2 On the server that will receive information, open a command window and type the following command:

`prserv` [*`listen_port`*]

where *listen_port* is the same port that you specified with the Nprintf parameter.

If you do not specify a port, 9001 is used by default.

While prserv is running, information from the Cisco IP Phone is sent to a file named *listen_port*.log, where *listen_port* is the port you specified with the Nprintf parameter and the prserv command. This file is stored on the server you specified with the Nprintf parameter in the folder from which you ran the prserv command. If the file exists, new information is appended to it.

You can open a *listen_port*.log file using a text editor.

Step 3 To exit prserv.exe and stop collecting information, press **Ctrl-C** in the command window.

Note If you want to collect information from more than one Cisco IP Phone, Cisco recommends that you store information in a separate *listen_port*.log file for each phone. If you store all information in a single file, it can be difficult to identify which messages belong to which phones. To generate separate *listen_port*.log files, configure each phone using its own profile or web page. For each phone, use the Nprintf parameter in the profile or web page to specify a unique port number on the server to which information will be sent. Then, run prserv.exe multiple times, once for each phone from which you want to collect information. Run each instance of prserv.exe in its own command window. For each instance, make sure to specify a port number that corresponds to a port number in a Nprintf parameter.

Related Topics

- General Troubleshooting Tips, page 9-1
- Resolving Problems, page 9-2
- Contacting TAC, page 9-5

Additional End User Features on the Cisco IP Phone Models 7905G and 7912G

This appendix describes Cisco IP Phone end user features that are not included in the current version of the Cisco IP Phone end user documentation. This information is provided here so that you can make it available to end users.

This appendix includes these topics:

- Call Preferences Menu, page A-1
- Softkeys, page A-6
- Other Features, page A-7

Call Preferences Menu

End users access the Call Preferences menu from the Settings menu on a Cisco IP Phone. What parameters appear on this menu and whether end users can change the value of a parameter depends on the Call Preference settings that you make for the phone in the profile or from the configuration web pages. For more information about configuring access to the Call Preferences menu and parameters, see the "Call Preference Parameters" section on page 8-13.

For information about editing parameter values, see the "Editing Parameter Values" section on page 5-5.

To display the Call Preferences menu, follow these steps:

Procedure

Step 1 Press the **Menu** button to access the Services menu.

Step 2 In the Services menu, use the **Navigation** button to select **Settings**, and then press the **Select** softkey.

Step 3 In the Settings menu, use the **Navigation** button to select **Call Preferences**, and then press the **Select** softkey.

To exit the Call Preferences menu, press the **Back** softkey until the **Exit** softkey appears, and then press the **Exit** softkey.

Table A-1 describes the parameters that can appear in the Call Preferences menu and explains how to change them.

Table A-1 Call Preference Menu Parameters

Parameter	Description	To Change
DisplayName	Specifies an alpha-numeric string that is used as part of the phone's caller ID and that appears on the phone's LCD screen. **Note** If the Block Caller ID parameter is set to Yes, outgoing calls will use "Anonymous" as the phone's caller ID regardless of the Display Name value.	1. Scroll to the DisplayName parameter, press the **Edit** softkey, and then enter a name. 2. Press the **Accept** softkey, and then press the **Save** softkey.
ShortName	Specifies a name to be displayed on the phone's LCD screen in place of the Display Name value. If the Short Name parameter is blank or set to 0, the Display Name value will be displayed. Short Name will not affect the Display Name value that is used as part of the phone's caller ID.	1. Scroll to the ShortName parameter, press the **Edit** softkey, and then enter a name. 2. Press the **Accept** softkey, and then press the **Save** softkey.

Table A-1 Call Preference Menu Parameters (continued)

Parameter	Description	To Change
Do Not Disturb	Specifies whether calls to the phone will receive a busy signal. When this parameter is set to Yes, the **DND** softkey becomes available on the phone. See the "Softkeys" section on page A-6 for more information.	1. Scroll to the Do Not Disturb parameter and press the **Yes** softkey to enable this parameter, or press the **No** softkey to disable it. 2. Press the **Save** softkey.
Allow Call Waiting	Specifies whether call waiting is enabled on the phone.	1. Scroll to the Allow Call Waiting parameter and press the **Yes** softkey to enable this parameter, or press the **No** softkey to disable it. 2. Press the **Save** softkey.
Block Caller ID	Specifies whether caller ID is blocked on outgoing calls. If this parameter is set to Yes, outgoing calls will use "Anonymous" as the phone's caller ID. If it is set to No, the phone's caller ID will include the Display Name value and phone number.	1. Scroll to the Block Caller ID parameter and press the **Yes** softkey to enable this parameter, or press the **No** softkey to disable it. 2. Press the **Save** softkey.
Block Anonymous Call	Specifies whether anonymous calls are rejected. If this parameter is set to Yes, incoming calls with "Anonymous" caller IDs will be rejected. If it is set to No, these calls will ring at the phone.	1. Scroll to the Block Anonymous Call parameter and press the **Yes** softkey to enable this parameter, or press the **No** softkey to disable it. 2. Press the **Save** softkey.
Allow Call Transfer	Specifies whether attended call transfers can be made from the phone. If this parameter is set to Yes, the **Trnsfer** softkey will appear when appropriate, allowing attended transfers of a calls. If this parameter is set to No, this softkey will never be available.	1. Scroll to the Allow Call Transfer parameter and press the **Yes** softkey to enable this parameter, or press the **No** softkey to disable it. 2. Press the **Save** softkey

Table A-1 Call Preference Menu Parameters (continued)

Parameter	Description	To Change
Allow Blind Transfer	Specifies whether blind call transfers can be made from the phone. If this parameter is set to Yes, the **BlndXfr** softkey will appear when appropriate, allowing blind transfers of calls. If this parameter is set to No, this softkey will never be available. See the "Other Features" section on page A-7 for more information about blind transfer.	1. Scroll to the Allow Blind Transfer parameter and press the **Yes** softkey to enable this parameter, or press the **No** softkey to disable it. 2. Press the **Save** softkey
Allow Conference	Specifies whether conference calls can be established from the phone. If this parameter is set to Yes, the **Confrn** softkey will appear when appropriate, allowing conference calls to be established. If this parameter is set to No, this softkey will never be available.	1. Scroll to the Allow Conference parameter and press the **Yes** softkey to enable this parameter, or press the **No** softkey to disable it. 2. Press the **Save** softkey
Time Format	Specifies the format for the time that appears on the phone's LCD screen. This format is specified by one or more of the following characters: h—designates the hour in 12-hour format H—designates the hour in 24-hour format i or I—designates minutes a or A—for 12-hour format, include "p" with times from noon until one minute before midnight : (colon)—displays a colon that blinks every second For example, when the current time is 1:30 P.M., • h:ia causes the time to appear as 1:30p. • H:I causes the time to appear as 13:30.	1. Scroll to the Time Format parameter, press the **Edit** softkey, and then enter a time format. 2. Press the **Accept** softkey, and then press the **Save** softkey.

Table A-1 Call Preference Menu Parameters (continued)

Parameter	Description	To Change
Date Format	Specifies the format for the date that appears on the phone's LCD screen. This format is specified by one or more of the following characters: m—designates the month as a number 1 through 12 M—designates the month as a three-letter abbreviation, Jan through Dec d or D—designates the day of the month y—designates a two-digit year (such as 03 for 2003) Y—designates a four-digit year Other characters—appear as entered For example, when the current date is March 10, 2003: • m-d-y causes the date to appear as 3-10-03. • M d, Y causes the date to appear as Mar 20, 2003. • Y/m/d causes the date to appear as 2003/3/10.	1. Scroll to the Date Format parameter, press the **Edit** softkey, and then enter a date format. 2. Press the **Accept** softkey, and then press the **Save** softkey.
Voice Mail Number	Specifies a phone number where voice messages are stored and retrieved. If a number is specified: • The **Message** softkey will appear when appropriate. • Incoming calls forward to this number if the phone is busy or if the calls are not answered within the number of seconds specified with the Forward to VMail Delay(s) parameter.	1. Scroll to the Voice Mail Number parameter, press the **Edit** softkey, and then enter a phone number. 2. Press the **Accept** softkey, and then press the **Save** softkey.

Table A-1 Call Preference Menu Parameters (continued)

Parameter	Description	To Change
Call Forward Number	Specifies a phone number to which all calls to the phone are forwarded. If a number is entered, the Call Forward All feature is activated.	1. Scroll to the Call Forward Number parameter, press the **Edit** softkey, and then enter a phone number. 2. Press the **Accept** softkey, and then press the **Save** softkey.
Forward to VMail Delay(s)	Specifies the number of seconds after which an incoming ringing call will be forwarded to the number specified by the Voice Mail Number parameter.	1. Scroll to the Forward to VMail Delay(s) parameter, press the **Edit** softkey, and then enter a value. 2. Press the **Accept** softkey, and then press the **Save** softkey.

Softkeys

Table A-2 describes the softkeys that can appear on the Cisco IP Phone models 7905G and 7912G and that are not described in the User Guide for the phone.

Table A-2 Sofkteys

Softkey	Description
Back	Displays the previous menu.
BlndXfr	Allows the blind transfer of a call when Allow Blind Transfer is enabled in the Call Preferences menu. In a blind transfer, you transfer a caller to another number without talking to the party who is to receive the call or verifying that the new party is there. To perform a blind transfer, follow these steps: 1. During a call, press the **More** soft key, then press the **BlndXfr** soft key. The call goes on hold. 2. Dial the number to which to transfer the call. The phone hangs up automatically.

Table A-2 Sofkteys (continued)

Softkey	Description
Clear	In the Call Preferences menu, clears the contents of the currently-displayed parameter.
Default	In the Call Preferences menu, changes the value of the currently-displayed parameter to its default value.
DND	Disables the Do Not Disturb feature and changes the setting of the Do Not Disturb parameter in the Call Preferences menu to No.
Drop	Allows the initiator of a conference call to disconnect the most recently connected active party in the call.
Factory	Changes volume and contrast settings to their default values. You access this softkey by pressing the **Menu** button, selecting Settings, and then pressing the **More** softkey.
Missed	Displays the Missed Calls directory.
Restore	Restores volume and contrast settings to the values currently stored in non-volatile memory on the phone. You access this softkey by pressing the **Menu** button, selecting Settings, and then pressing the **More** softkey.

Other Features

Table A-3 describes features on the Cisco IP Phone models 7905G and 7912G that are not described elsewhere in this appendix or in the User Guide for the phone.

Table A-3 Other Features

Feature	Description
Ringer sound	The ringer sound cannot be changed on the phone.
Stutter tone for message waiting	In addition to lighting the red light on the handset, the Cisco IP Phone plays a stutter tone to indicate one or more new voice mail messages. A stutter tone is a series of short dial tones that a user hears instead of a regular dial tone when placing a call.

Phone Menu, Web Page, and Profile Equivalent Parameters

Table B-1 shows the configurable parameters on the phone menus and their equivalent parameters in the phone configuration web pages and profile.

Table B-1 Phone Menu, Web Page and Profile Parameters

Phone Menu Parameter	Phone Web Page and Profile Parameter
Admin. VLAN Id	VLANSetting
Alternate DNS	DNS2IP
Alternate NTP	AltNTPIP
Alternate TFTP	TftpURL
Backup Proxy Timeout	AltProxyTimeOut
CDP Enabled	OpFlags
Default Router	StaticRoute
DHCP Enabled	Dhcp
DNS Server 1	DNS1IP
DNS Server 2	DNS2IP
Domain (if the Alternate Domain option is set to yes)	Domain
IP Address	StaticIP
Local RTP Port	MediaPort

Table B-1 Phone Menu, Web Page and Profile Parameters (continued)

Phone Menu Parameter	Phone Web Page and Profile Parameter
Local SIP Port	SIPPort
Login ID	LoginID
NAT WAN IP Address	NATIP
NTP Server 1	NTPIP
NTP Server 2	AltNTPIP
Outbound Proxy	OutboundProxy
Password	PWD
Profile Encrypt Key	EncryptKey
Register Expires	SipRegInterval
Register with Proxy	SipRegOn
SIP Proxy	Proxy
Subnet Mask	StaticNetMask
TFTP Enabled	UseTftp
TFTP Server	TftpURL
Time Zone	TimeZone
Use Login ID	UseLoginID
User ID	UID
VLAN Enabled	OpFlags

SIP Call Flows

This appendix describes some basic call flows for the Cisco IP Phone models 7905G and 7912G. It includes the following sections:

- Supported SIP Request Methods, page C-1
- Call Flow Scenarios for Successful Calls, page C-2

Supported SIP Request Methods

The Cisco IP Phone supports the following SIP request methods:

- INVITE—Indicates a user or service is being invited to participate in a call session.
- ACK—Confirms that the client has received a final response to an INVITE request.
- BYE—Terminates a call and can be sent by either the caller or the callee.
- CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.
- REGISTER—Registers the address listed in the To header field with a SIP proxy.
- NOTIFY—Notifies the user of the status of a transfer using REFER. Also used for remote reset and for message waiting.
- OPTIONS—Provides requestors with SIP methods and codecs supported by the phone.

The following types of responses are used by SIP and generated by the Cisco SIP gateway:

- SIP 1*xx*—Informational responses
- SIP 2*xx*—Successful responses
- SIP 3*xx*—Redirection responses
- SIP 4*xx*—Client Failure responses
- SIP 5*xx*—Server Failure responses
- SIP 6*xx*—Global Failure responses

Call Flow Scenarios for Successful Calls

This section describes call flows for the following scenarios:

- Cisco IP Phone-to-SIP Server—Registration without Authentication, page C-2
- Cisco IP Phone-to-SIP Server—Registration with Authentication, page C-4
- Cisco IP Phone-to-Cisco IP Phone—Basic SIP to SIP Call without Authentication, page C-7
- Cisco IP Phone-to-Cisco IP Phone—Basic SIP to SIP Call with Authentication, page C-15

Each of the call flows includes a call diagram, action descriptions table, and a sample log file.

Cisco IP Phone-to-SIP Server—Registration without Authentication

Figure C-1 illustrates the Cisco IP Phone registering with the SIP server where authentication is not required for registration. Table C-1 describes these actions in detail. Table C-2 shows the log of these actions.

The call flow is as follows:

1. Cisco IP Phone requests registration.
2. Registration is completed.

Figure C-1 Cisco IP Phone-to-SIP Server—Registration without Authentication

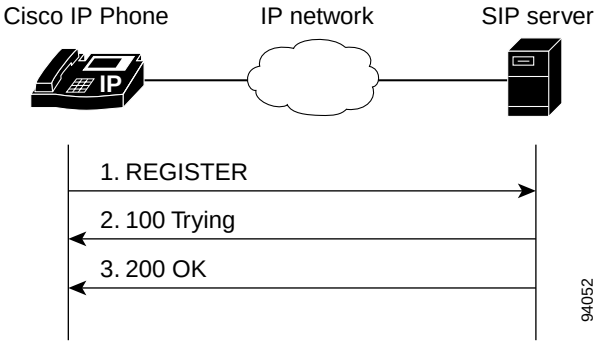


Table C-1 Action Descriptions

Step	Action	Description
Step 1	REGISTER—Cisco IP Phone to SIP server	Cisco IP Phone sends a REGISTER message to the SIP server to register the address in the To header field.
Step 2	100 Trying—SIP Server to Cisco IP Phone	SIP server returns a 100 Trying message, indicating that the REGISTER request has been received.
Step 3	200 OK—SIP server to Cisco IP Phone	SIP server returns a final 200 OK response, confirming that registration is complete.

Table C-2 Log Listing

1.	REGISTER sip:cisco.com SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=1692201497 To: <sip:9313@cisco.com;user=phone> Call-ID: 2923175725@192.168.2.163 CSeq: 1 REGISTER Contact: <sip:9313@192.168.2.163:5060;user=phone;transport=udp>;expires=3600 User-Agent: Cisco-CP7905/1.01-030429A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0
2.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 Call-ID: 2923175725@192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=1692201497 To: <sip:9313@cisco.com;user=phone> CSeq: 1 REGISTER Content-Length: 0
3.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 Call-ID: 2923175725@192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=1692201497 To: <sip:9313@cisco.com;user=phone> CSeq: 1 REGISTER Contact: <sip:9313@192.168.2.163:5060;user=phone;transport=udp>;expires="Fri, 02 May 2003 00:52:58 GMT" Expires: 3600 Content-Length: 0

Cisco IP Phone-to-SIP Server—Registration with Authentication

Figure C-2 illustrates the Cisco IP Phone registering with the SIP server where authentication is required for registration. Table C-3 describes these actions in detail. Table C-4 shows the log of these actions.

The call flow is as follows:

1. Cisco IP Phone requests registration.
2. SIP server requests authentication credential.
3. Authentication is received and registration is completed.

Figure C-2 Cisco IP Phone-to-SIP Server—Registration with Authentication

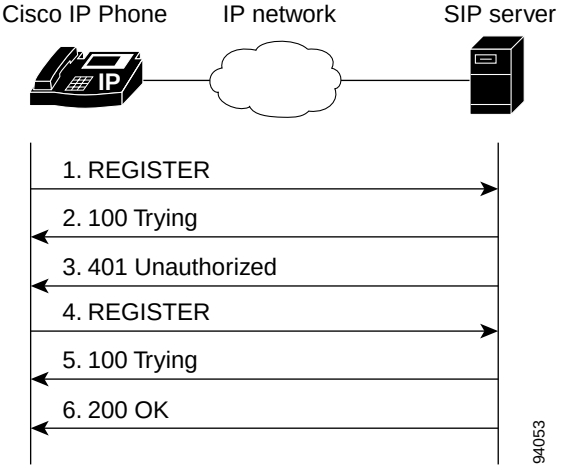


Table C-3 Action Descriptions

Step	Action	Description
Step 1	REGISTER—Cisco IP Phone to SIP server	Cisco IP Phone sends a REGISTER message to the SIP server to register the address in the To header field.
Step 2	100 Trying—SIP server to Cisco IP Phone	SIP server returns a 100 trying message, indicating that the REGISTER request has been received.
Step 3	401 Unauthorized— SIP server to Cisco IP Phone	SIP server returns a request for authentication.
Step 4	REGISTER—Cisco IP Phone to SIP server	Cisco IP Phone attempts to register using its authentication credential.
Step 5	100 Trying—SIP server to Cisco IP Phone	SIP server returns a 100 trying message, indicating that the new REGISTER request has been received.
Step 6	200 OK—SIP server to Cisco IP Phone	SIP server returns a final 200 OK response, confirming that the authentication credential has been verified and registration is complete.

Table C-4 Log Listing

1.	REGISTER sip:cisco.com SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=118440597 To: <sip:9313@cisco.com;user=phone> Call-ID: 948614169@192.168.2.163 CSeq: 1 REGISTER Contact: <sip:9313@192.168.2.163:5060;user=phone;transport=udp>;expires=3600 User-Agent: Cisco-CP7905/1.01-030429A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0
2.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 Call-ID: 948614169@192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=118440597 To: <sip:9313@cisco.com;user=phone> CSeq: 1 REGISTER Content-Length: 0
3.	SIP/2.0 401 Unauthorized Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 Call-ID: 948614169@192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=118440597 To: <sip:9313@cisco.com;user=phone> CSeq: 1 REGISTER WWW-Authenticate: DIGEST realm="CISCO", nonce="3eb1ad3b", algorithm=MD5 Content-Length: 0
4.	REGISTER sip:cisco.com SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=118440597 To: <sip:9313@cisco.com;user=phone> Call-ID: 948614169@192.168.2.163 CSeq: 2 REGISTER Contact: <sip:9313@192.168.2.163:5060;user=phone;transport=udp>;expires=3600 User-Agent: Cisco-CP7905/1.01-030429A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Authorization: Digest username="9313",realm="CISCO",nonce="3eb1ad3b",uri="sip:cisco.com",response="e52 5065aac09e798058122020e3d1921" Content-Length: 0

Table C-4 Log Listing (continued)

5.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 Call-ID: 948614169@192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=118440597 To: <sip:9313@cisco.com;user=phone> CSeq: 2 REGISTER Content-Length: 0
6.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 Call-ID: 948614169@192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=118440597 To: <sip:9313@cisco.com;user=phone> CSeq: 2 REGISTER Contact: <sip:9313@192.168.2.163:5060;user=phone;transport=udp>;expires="Fri, 02 May 2003 00:26:51 GMT" Expires: 3600 Content-Length: 0

Cisco IP Phone-to-Cisco IP Phone—Basic SIP to SIP Call without Authentication

Figure C-3 illustrates a call from one Cisco IP Phone to another where authentication by the SIP server is not required. Table C-5 describes these actions in detail. Table C-6 shows the log of these actions.

The call flow is as follows:

1. Call is established between Cisco IP Phone A and Cisco Cisco IP Phone B.
2. Call is terminated.

Figure C-3 Cisco IP Phone-to-Cisco IP Phone—Basic SIP to SIP Call without Authentication

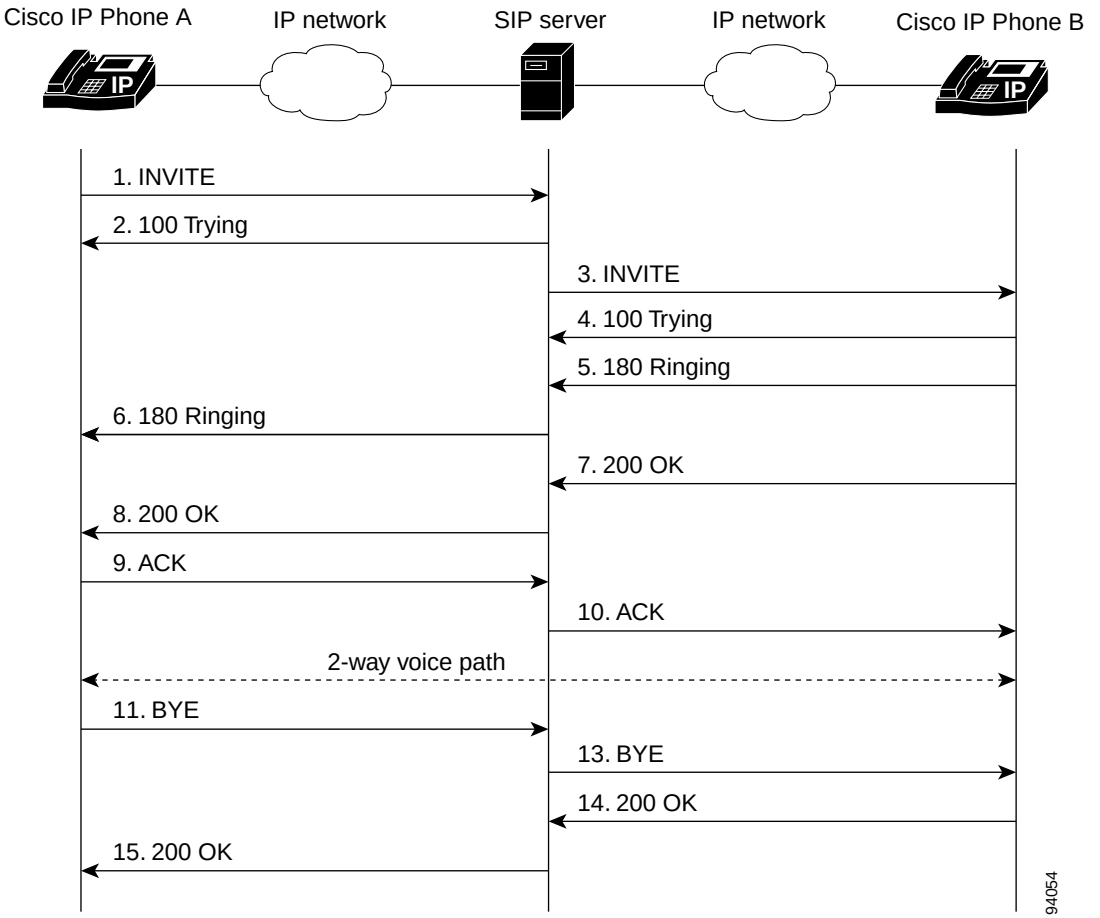


Table C-5 Action Descriptions

Step	Action	Description
Step 1	INVITE—Cisco IP Phone A to SIP server	Cisco IP Phone A sends a call session INVITE request to the SIP server to pass on to Cisco IP Phone B.
Step 2	100 Trying—SIP server to Cisco IP Phone A	SIP server returns a 100 trying message, indicating that the INVITE request has been received.
Step 3	INVITE—SIP server to Cisco IP Phone B	SIP server sends the call session INVITE request to Cisco IP Phone B.
Step 4	100 Trying—Cisco IP Phone B to SIP server	Cisco IP Phone B returns a 100 trying message indicating that the INVITE request has been received.
Step 5	180 Ringing—Cisco IP Phone B to SIP server	Cisco IP Phone B sends a 180 ringing response to the SIP server to pass on to Cisco IP Phone A.
Step 6	180 Ringing—SIP server to Cisco IP Phone A	SIP server sends the 180 ringing response to Cisco IP Phone A.
Step 7	200 OK—Cisco IP Phone B to SIP server	Cisco IP Phone B sends a 200 OK message to the SIP server indicating that a connection has been established.
Step 8	200 OK—SIP server to Cisco IP Phone A	SIP server passes the 200 OK message to Cisco IP Phone A.
Step 9	ACK—Cisco IP Phone A to SIP server	Cisco IP Phone A sends acknowledgement of the 200 OK response to the SIP server to pass on to Cisco IP Phone B.
Step 10	ACK—SIP server to Cisco IP Phone B	SIP server passes ACK response to Cisco IP Phone B.
A two-way voice path is established between Cisco IP Phone A and Cisco IP Phone B.		
Step 11	BYE—Cisco IP Phone A to SIP server	Cisco IP Phone A terminates the call session and sends a BYE request to the SIP server indicating that Cisco IP Phone A wants to terminate the call.

Table C-5 Action Descriptions (continued)

Step	Action	Description
Step 12	BYE—SIP server to Cisco IP Phone B	SIP server passes the BYE request to Cisco IP Phone B.
Step 13	200 OK—Cisco IP Phone B to SIP server	Cisco IP Phone B sends a 200 OK message to the SIP server indicating that Cisco IP Phone B has received the BYE request.
Step 14	200 OK—SIP server to Cisco IP Phone A	SIP server passes the BYE request to Cisco IP Phone A.

Table C-6 Log Listing

1.	`INVITE sip:9314@cisco.com;user=phone SIP/2.0`
	`Via: SIP/2.0/UDP 192.168.2.163:5060`
	`From: <sip:9313@cisco.com;user=phone>;tag=2274744465`
	`To: <sip:9314@cisco.com;user=phone>`
	`Call-ID: 4074632257@192.168.2.163`
	`CSeq: 1 INVITE`
	`Contact: <sip:9313@192.168.2.163:5060;user=phone;transport=udp>`
	`User-Agent: Cisco-CP7905/1.01-030429A`
	`Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER`
	`Expires: 300`
	`Content-Length: 259`
	`Content-Type: application/sdp`
	
	`v=0`
	`o=9313 58115 58115 IN IP4 192.168.2.163`
	`s=Cisco 7905 SIP Call`
	`c=IN IP4 192.168.2.163`
	`t=0 0`
	`m=audio 16384 RTP/AVP 0 18 8 101`
	`a=rtpmap:0 PCMU/8000/1`
	`a=rtpmap:18 G729/8000/1`
	`a=rtpmap:8 PCMA/8000/1`
	`a=rtpmap:101 telephone-event/8000`
	`a=fmtp:101 0-15`

Table C-6 Log Listing (continued)

2.

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163
Call-ID: 4074632257@192.168.2.163
From: <sip:9313@cisco.com;user=phone>;tag=2274744465
To: <sip:9314@cisco.com;user=phone>
CSeq: 1 INVITE
Content-Length: 0
```

3.

```
INVITE sip:9314@192.168.3.232:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 192.168.2.97:5060;branch=5b495e54-d5a8a93e-aa5f9258-be025820-1
Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163
From: <sip:9313@cisco.com;user=phone>;tag=2274744465
To: <sip:9314@cisco.com;user=phone>
Call-ID: 4074632257@192.168.2.163
CSeq: 1 INVITE
Contact: <sip:9313@192.168.2.163:5060;user=phone;transport=udp>
User-Agent: Cisco-CP7905/1.01-030429A
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER
Expires: 300
Content-Length: 259
Content-Type: application/sdp

v=0
o=9313 58115 58115 IN IP4 192.168.2.163
s=Cisco 7905 SIP Call
c=IN IP4 192.168.2.163
t=0 0
m=audio 16384 RTP/AVP 0 18 8 101
a=rtpmap:0 PCMU/8000/1
a=rtpmap:18 G729/8000/1
a=rtpmap:8 PCMA/8000/1
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

4.

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.2.97:5060;branch=5b495e54-d5a8a93e-aa5f9258-be025820-1
Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163
From: <sip:9313@cisco.com;user=phone>;tag=2274744465
To: <sip:9314@cisco.com;user=phone>;tag=252438364
Call-ID: 4074632257@192.168.2.163
CSeq: 1 INVITE
Server: Cisco-CP7905/1.01-030422A
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER
Content-Length: 0
```

Table C-6 Log Listing (continued)

5.	SIP/2.0 180 Ringing Via: SIP/2.0/UDP 192.168.2.97:5060;branch=5b495e54-d5a8a93e-aa5f9258-be025820-1 Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=2274744465 To: <sip:9314@cisco.com;user=phone>;tag=252438364 Call-ID: 4074632257@192.168.2.163 CSeq: 1 INVITE Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0
6.	SIP/2.0 180 Ringing Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=2274744465 To: <sip:9314@cisco.com;user=phone>;tag=252438364 Call-ID: 4074632257@192.168.2.163 CSeq: 1 INVITE Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0
7.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.97:5060;branch=5b495e54-d5a8a93e-aa5f9258-be025820-1 Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=2274744465 To: <sip:9314@cisco.com;user=phone>;tag=252438364 Call-ID: 4074632257@192.168.2.163 CSeq: 1 INVITE Contact: <sip:9314@192.168.3.232:5060;user=phone;transport=udp> Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 205 Content-Type: application/sdp v=0 o=9314 58362 58362 IN IP4 192.168.3.232 s=Cisco 7905 SIP Call c=IN IP4 192.168.3.232 t=0 0 m=audio 16384 RTP/AVP 0 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15

Table C-6 Log Listing (continued)

8.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=2274744465 To: <sip:9314@cisco.com;user=phone>;tag=252438364 Call-ID: 4074632257@192.168.2.163 CSeq: 1 INVITE Contact: <sip:9314@192.168.3.232:5060;user=phone;transport=udp> Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 205 Content-Type: application/sdp v=0 o=9314 58362 58362 IN IP4 192.168.3.232 s=Cisco 7905 SIP Call c=IN IP4 192.168.3.232 t=0 0 m=audio 16384 RTP/AVP 0 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15
9.	ACK sip:9314@192.168.3.232;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=2274744465 To: <sip:9314@cisco.com;user=phone>;tag=252438364 Call-ID: 4074632257@192.168.2.163 CSeq: 1 ACK User-Agent: Cisco-CP7905/1.01-030429A Content-Length: 0
10.	ACK sip:9314@192.168.3.232;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=2274744465 To: <sip:9314@cisco.com;user=phone>;tag=252438364 Call-ID: 4074632257@192.168.2.163 CSeq: 1 ACK User-Agent: Cisco-CP7905/1.01-030429A Content-Length: 0

Table C-6 Log Listing (continued)

11.	BYE sip:9314@192.168.3.232;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=2274744465 To: <sip:9314@cisco.com;user=phone>;tag=252438364 Call-ID: 4074632257@192.168.2.163 CSeq: 2 BYE User-Agent: Cisco-CP7905/1.01-030429A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0
12.	BYE sip:9314@192.168.3.232;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=2274744465 To: <sip:9314@cisco.com;user=phone>;tag=252438364 Call-ID: 4074632257@192.168.2.163 CSeq: 2 BYE User-Agent: Cisco-CP7905/1.01-030429A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0
13.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=2274744465 To: <sip:9314@cisco.com;user=phone>;tag=252438364 Call-ID: 4074632257@192.168.2.163 CSeq: 2 BYE Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0
14.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=2274744465 To: <sip:9314@cisco.com;user=phone>;tag=252438364 Call-ID: 4074632257@192.168.2.163 CSeq: 2 BYE Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0

Cisco IP Phone-to-Cisco IP Phone—Basic SIP to SIP Call with Authentication

Figure C-4 illustrates a call from one Cisco IP Phone to another where authentication by the SIP server is required. Table C-7 describes these actions in detail. Table C-8 shows the log of these actions.

The call flow is as follows:

1. Authentication is requested for call initiated by Cisco IP Phone A.
2. Call is established between Cisco IP Phone A and Cisco IP Phone B.
3. Call is terminated.

Figure C-4 Cisco IP Phone-to-Cisco IP Phone—Basic SIP to SIP Call with Authentication

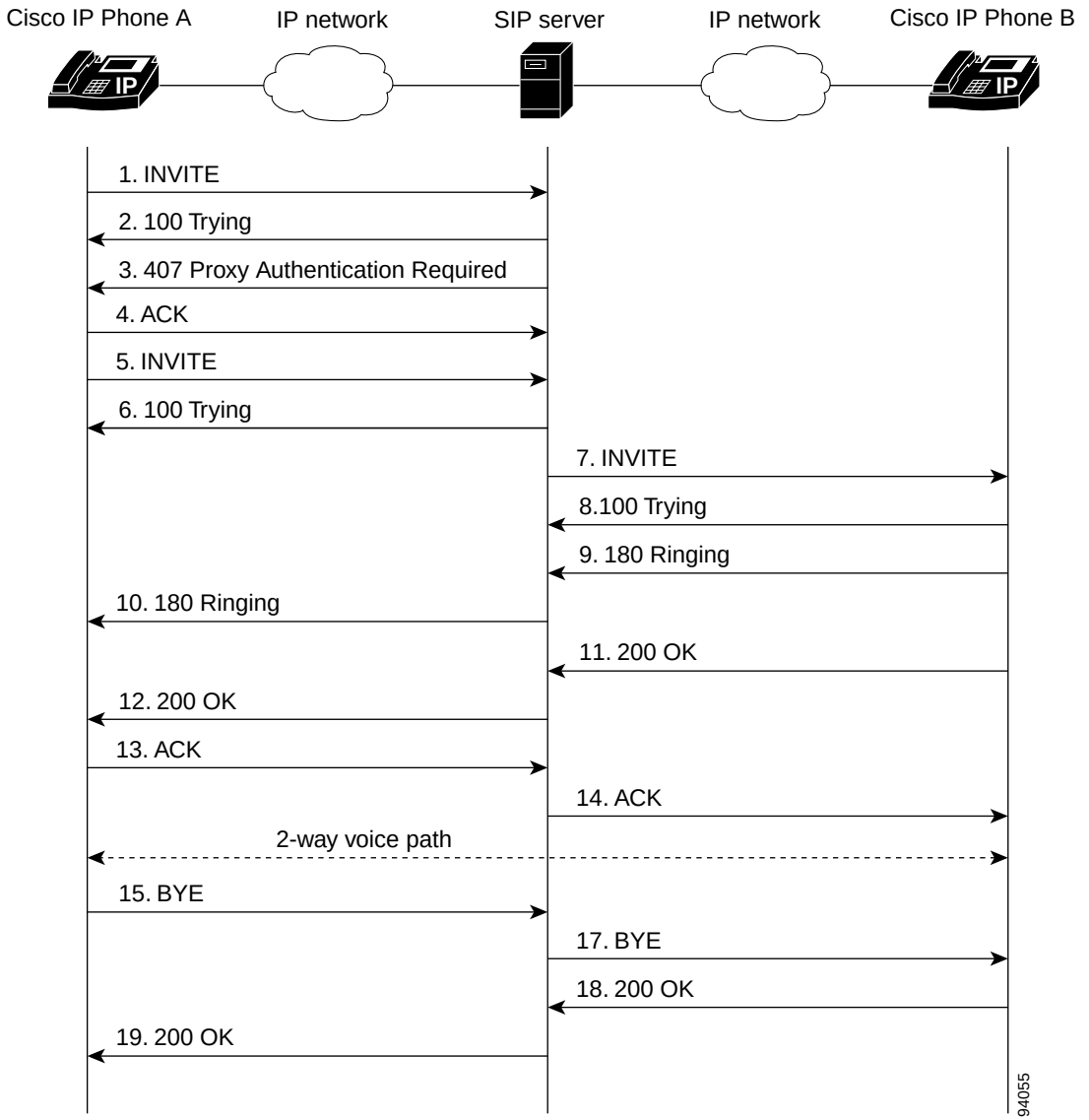


Table C-7 Action Descriptions

Step	Action	Description
Step 1	INVITE—Cisco IP Phone A to SIP server	Cisco IP Phone A sends a call session INVITE request to the SIP server to pass on to Cisco IP Phone B.
Step 2	100 Trying—SIP server to Cisco IP Phone A	SIP server returns a 100 Trying message, indicating that the INVITE request has been received.
Step 3	407 Proxy Authentication Required— SIP server to Cisco IP Phone A	SIP server returns a request for authentication to Cisco IP Phone A.
Step 4	ACK—Cisco IP Phone A to SIP server	Cisco IP Phone A acknowledges the request for authentication.
Step 5	INVITE—Cisco IP Phone A to SIP server	Cisco IP Phone A sends a call session INVITE request along with authentication credential to the SIP server to pass on to Cisco IP Phone B.
Step 6	100 Trying—SIP server to Cisco IP Phone A	SIP server returns a 100 Trying message, indicating that the INVITE request has been received.
Step 7	INVITE—SIP server to Cisco IP Phone B	SIP server sends the call session INVITE request to Cisco IP Phone B.
Step 8	100 Trying—Cisco IP Phone B to SIP server	Cisco IP Phone B returns a 100 trying message indicating that the INVITE request has been received.
Step 9	180 Ringing—Cisco IP Phone B to SIP server	Cisco IP Phone B sends a 180 ringing response to the SIP server to pass on to Cisco IP Phone A.
Step 10	180 Ringing—SIP server to Cisco IP Phone A	SIP server sends the 180 ringing response to Cisco IP Phone A.
Step 11	200 OK—Cisco IP Phone B to SIP server	Cisco IP Phone B sends a 200 OK message to the SIP server indicating that a connection has been established.
Step 12	200 OK—SIP server to Cisco IP Phone A	SIP server passes the 200 OK message to Cisco IP Phone A.

Table C-7 Action Descriptions (continued)

Step	Action	Description
Step 13	ACK—Cisco IP Phone A to SIP server	Cisco IP Phone A sends acknowledgment of the 200 OK response to the SIP server to pass on to Cisco IP Phone B.
Step 14	ACK—SIP server to Cisco IP Phone B	SIP server passes ACK response to Cisco IP Phone B.
A two-way voice path is established between Cisco IP Phone A and Cisco IP Phone B.		
Step 15	BYE—Cisco IP Phone A to SIP server	Cisco IP Phone A terminates the call session and sends a BYE request to the SIP server indicating that Cisco IP Phone A wants to terminate the call.
Step 16	BYE—SIP server to Cisco IP Phone B	SIP server passes the BYE request to Cisco IP Phone B.
Step 17	200 OK—Cisco IP Phone B to SIP server	Cisco IP Phone 186 B sends a 200 OK message to the SIP server indicating that Cisco IP Phone 186 B has received the BYE request.
Step 18	200 OK—SIP server to Cisco IP Phone A	SIP server passes the BYE request to Cisco IP Phone A.

Table C-8 Log Listing

1.	INVITE sip:9314@cisco.com;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone> Call-ID: 2765277948@192.168.2.163 CSeq: 1 INVITE Contact: <sip:9313@192.168.2.163:5060;user=phone;transport=udp> User-Agent: Cisco-CP7905/1.01-030429A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Expires: 300 Content-Length: 257 Content-Type: application/sdp v=0 o=9313 8737 8737 IN IP4 192.168.2.163 s=Cisco 7905 SIP Call c=IN IP4 192.168.2.163 t=0 0 m=audio 16384 RTP/AVP 0 18 8 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:18 G729/8000/1 a=rtpmap:8 PCMA/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15
2.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 Call-ID: 2765277948@192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone> CSeq: 1 INVITE Content-Length: 0
3.	SIP/2.0 407 Proxy Authentication Required Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 Call-ID: 2765277948@192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=4d241cc8-1145efd4 CSeq: 1 INVITE Proxy-Authenticate: DIGEST realm="CISCO", nonce="3eb1be0a", algorithm=MD5 Content-Length: 0

Table C-8 Log Listing (continued)

4.	ACK sip:9314@cisco.com;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=4d241cc8-1145efd4 Call-ID: 2765277948@192.168.2.163 CSeq: 1 ACK User-Agent: Cisco-CP7905/1.01-030429A Content-Length: 0
5.	INVITE sip:9314@cisco.com;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone> Call-ID: 2765277948@192.168.2.163 CSeq: 2 INVITE Contact: <sip:9313@192.168.2.163:5060;user=phone;transport=udp> User-Agent: Cisco-CP7905/1.01-030429A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Proxy-Authorization: Digest username="9313",realm="CISCO",nonce="3eb1be0a",uri="sip:9314@cisco.com",response ="40190e28f6f098437e4a7edcd73c4ce6" Expires: 300 Content-Length: 257 Content-Type: application/sdp v=0 o=9313 8749 8749 IN IP4 192.168.2.163 s=Cisco 7905 SIP Call c=IN IP4 192.168.2.163 t=0 0 m=audio 16384 RTP/AVP 0 18 8 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:18 G729/8000/1 a=rtpmap:8 PCMA/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15
6.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 Call-ID: 2765277948@192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone> CSeq: 2 INVITE Content-Length: 0

Table C-8 Log Listing (continued)

7.	INVITE sip:9314@192.168.3.232:5060;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.97:5060;branch=fa2b71c3-292cb31a-a4158bcf-2cb346be-1 Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone> Call-ID: 2765277948@192.168.2.163 CSeq: 2 INVITE Contact: <sip:9313@192.168.2.163:5060;user=phone;transport=udp> User-Agent: Cisco-CP7905/1.01-030429A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Expires: 300 Content-Length: 257 Content-Type: application/sdp v=0 o=9313 8749 8749 IN IP4 192.168.2.163 s=Cisco 7905 SIP Call c=IN IP4 192.168.2.163 t=0 0 m=audio 16384 RTP/AVP 0 18 8 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:18 G729/8000/1 a=rtpmap:8 PCMA/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15
8.	SIP/2.0 100 Trying Via: SIP/2.0/UDP 192.168.2.97:5060;branch=fa2b71c3-292cb31a-a4158bcf-2cb346be-1 Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 2 INVITE Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0
9.	SIP/2.0 180 Ringing Via: SIP/2.0/UDP 192.168.2.97:5060;branch=fa2b71c3-292cb31a-a4158bcf-2cb346be-1 Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 2 INVITE Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0

Table C-8 Log Listing (continued)

10.	SIP/2.0 180 Ringing Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 2 INVITE Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0
11.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.97:5060;branch=fa2b71c3-292cb31a-a4158bcf-2cb346be-1 Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 2 INVITE Contact: <sip:9314@192.168.3.232:5060;user=phone;transport=udp> Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 203 Content-Type: application/sdp v=0 o=9314 8644 8644 IN IP4 192.168.3.232 s=Cisco 7905 SIP Call c=IN IP4 192.168.3.232 t=0 0 m=audio 16384 RTP/AVP 0 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15

Table C-8 Log Listing (continued)

12.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.163:5060;received=192.168.2.163 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 2 INVITE Contact: <sip:9314@192.168.3.232:5060;user=phone;transport=udp> Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 203 Content-Type: application/sdp v=0 o=9314 8644 8644 IN IP4 192.168.3.232 s=Cisco 7905 SIP Call c=IN IP4 192.168.3.232 t=0 0 m=audio 16384 RTP/AVP 0 101 a=rtpmap:0 PCMU/8000/1 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15
13.	ACK sip:9314@192.168.3.232;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 2 ACK User-Agent: Cisco-CP7905/1.01-030429A Proxy-Authorization: Digest username="9313",realm="CISCO",nonce="3eb1be0a",uri="sip:9314@cisco.com",response ="40190e28f6f098437e4a7edcd73c4ce6" Content-Length: 0
14.	ACK sip:9314@192.168.3.232;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 2 ACK User-Agent: Cisco-CP7905/1.01-030429A Proxy-Authorization: Digest username="9313",realm="CISCO",nonce="3eb1be0a",uri="sip:9314@cisco.com",response [0]DPKT 1st: 800 560, pt 13 ="40190e28f6f098437e4a7edcd73c4ce6" Content-Length: 0

Table C-8 Log Listing (continued)

15.	BYE sip:9314@192.168.3.232;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 3 BYE User-Agent: Cisco-CP7905/1.01-030429A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Proxy-Authorization: Digest username="9313",realm="CISCO",nonce="3eb1be0a",uri="sip:9314@cisco.com",response ="8b95de72274483131516ebb2b4086d71" Content-Length: 0
16.	BYE sip:9314@192.168.3.232;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 3 BYE User-Agent: Cisco-CP7905/1.01-030429A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Proxy-Authorization: Digest username="9313",realm="CISCO",nonce="3eb1be0a",uri="sip:9314@cisco.com",response ="8b95de72274483131516ebb2b4086d71" Content-Length: 0
17.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 3 BYE Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0
18.	SIP/2.0 200 OK Via: SIP/2.0/UDP 192.168.2.163:5060 From: <sip:9313@cisco.com;user=phone>;tag=3907367229 To: <sip:9314@cisco.com;user=phone>;tag=338213918 Call-ID: 2765277948@192.168.2.163 CSeq: 3 BYE Server: Cisco-CP7905/1.01-030422A Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER Content-Length: 0

Specifications for the Cisco IP Phone Models 7905G and 7912G

This appendix provides specifications for the Cisco IP Phone models 7905G and 7912G. It contains the following sections:

- Physical Specifications, page D-2
- Electrical Specifications, page D-2
- Environmental Specifications, page D-3
- Physical Interfaces, page D-3
- Software Specifications, page D-3

Physical Specifications

Table D-1 Cisco IP Phone models 7905G and 7912G Physical Specifications

Description	Specification
Dimensions	Length: 8.5 in. (21.7 cm) Width: 7.0 in. (17.8 cm) Depth: 3.8 in. (9.5 cm) without snap-on base or 5.9 in. (14.9 cm) with base
Weight	2.0 lb (0.9 kg)

Electrical Specifications

Table D-2 Cisco IP Phone models 7905G and 7912G Electrical Specifications

Description	Specification
Power	2.5 to 3.5W (idle to peak)
DC input voltage	+48 VDC at 1.5A maximum
Power adaptor	Universal AC/DC ~3.3 x 2.0 x 1.3 in. (~8.5 x 5.0 x 3.2 cm) ~4.8 oz (135 g) for the AC-input external power adaptor ~4 ft (1.2 m) DC cord 6 ft (1.8 m) cord UL/CUL, CE approved Class II transformer

Environmental Specifications

Table D-3 Cisco IP Phone models 7905G and 7912G Environmental Specifications

Description	Specification
Operating temperature	41 to 104°F (5 to 40°C)
Storage temperature	–4 to 140°F (–20 to 65°C)
Relative humidity	10 to 90% noncondensing, operating, and nonoperating/storage

Physical Interfaces

Table D-4 Cisco IP Phone models 7905G and 7912G Physical Interfaces

Description	Specification
Ethernet	RJ-45 8-wire connector, IEEE 802.3 10BASE-T standard
Power	48-VDC power connector

Software Specifications

Table D-5 Cisco IP Phone models 7905G and 7912G Software Specifications

Description	Specification
Voice-over-IP (VoIP) protocols	SIP (RFC 2543)
Voice coder-decoders (codecs)	G.729, G.729A, G.729AB G.711 A-law G.711 u-law

Table D-5 Cisco IP Phone models 7905G and 7912G Software Specifications

Description	Specification
Provisioning and configuration	DHCP (RFC 2131) Web configuration via built-in web server Basic boot provisioning (RFC 1350 TFTP Profiling) Dial plan provisioning Cisco Discovery Protocol (CDP)
Security	RC4 encryption for TFTP configuration profiles
Call progress tones	Configurable for up to two sets of frequencies and multiple on/off cadences
Voice features	Voice activity detection (VAD) Comfort noise generation (CNG) Dynamic jitter buffer (adaptive)

Numerics

10BASE-T 110-Mbps baseband Ethernet specification using two pairs of twisted-pair cabling (Categories 3, 4, or 5): one pair for transmitting data and the other for receiving data. 10BASE-T, which is part of the IEEE 802.3 specification, has a distance limit of approximately 328 feet (100 meters) per segment.

A

A-law ITU-T companding standard used in the conversion between analog and digital signals in PCM systems. A-law is used primarily in European telephone networks and is similar to the North American u-law standard. See also companding and u-law.

B

BTXML Basic Telephony Extensible Markup Language. See XML.

C

category x cable One of five grades of UTP cabling described in the EIA/TIA-586 standard. Category 3 cabling is used in 10BASE-T networks and can transmit data at speeds up to 10 Mbps. Category 5 cabling can transmit data at speeds up to 100 Mbps.

CDP Cisco Discovery Protocol. Used primarily to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media- and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

CED tone CallED station identification. A 3-second, 2100-Hz tone generated by a fax machine while answering a call, which is used in the handshaking used to set the call; the response from a called fax machine to a CNG tone.

CELP Code excited linear prediction compression. Compression algorithm used in low bit-rate voice encoding. Used in ITU-T Recommendations G.728, G.729, and G.723.1.

CLIP Calling Line Identification Presentation. Shows your identity to callers with Caller ID.

CLIR Calling Line Identification Restriction. Hides your identity from callers with Caller ID.

CNG Comfort noise generation or calling tone. Distinctive, repeating 1100-Hz tone (on for 0.5 seconds, off for 3 seconds) generated by a fax machine when placing a call.

codec Coder-decoder. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm used to compress/decompress speech or audio signals.

companding Contraction derived from the opposite processes of compression and expansion. Part of the PCM process whereby analog signal values are rounded logically to discrete scale-step values on a nonlinear scale. The decimal step number then is coded in its binary equivalent before transmission. The process is reversed at the receiving terminal using the same nonlinear scale. Compare with compression and expansion. See also A-law and u-law.

compression The running of a data set through an algorithm that reduces the space required to store or the bandwidth required to transmit the data set. Compare with companding and expansion.

CoS Class of service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. In SNA subarea routing, CoS definitions are used by subarea nodes to determine the optimal route to establish a given session. A CoS definition comprises a virtual route number and a transmission priority field. Also called ToS.

D

DHCP Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

dial peer An addressable call endpoint. In Voice over IP (VoIP), there are two types of dial peers: POTS and VoIP.

DNS Domain Name System. System used on the Internet for translating names of network nodes into IP addresses.

DSL Digital subscriber line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.

DSP Digital signal processor. Specialized hardware and software algorithms that perform complex processing of digitized data that was originally analog data. Typically segments a voice signal into frames and stores the frames in voice packets.

DTMF Dual tone multifrequency. A type of signaling that combines two distinct frequencies to generate a tone for each digit or character dialed, which is used by customers to signal the network. Sometimes referred to as “touchtone,” because a customer generally touches keypad keys to generate the tones.

E

E.164 The international public telecommunications numbering plan. A standard set by the ITU-T that addresses telephone numbers.

endpoint A source or sink of voice data, which may be physical (such as a trunk interface or a line interface in a media gateway) or logical (such as an announcement stored on a server).

expansion The process of running a compressed data set through an algorithm that restores the data set to its original size. Compare with companding and compression.

F

firewall Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

FQDN Fully qualified domain name. FQDN is the full name of a system, including the domain name and not just the host name. For example, aldebaran is a host name, and aldebaran.interop.com is an FQDN.

FSK Frequency shift key.

FXO Foreign exchange office. An FXO interface connects to the public switched telephone network (PSTN) central office and is the interface offered on a standard telephone. The Cisco FXO interface is an RJ-11 connector that allows an analog connection at the PSTN central office or to a station interface on a PBX.

FXS Foreign exchange station. An FXS interface connects directly to a standard telephone and supplies ring, voltage, and dial tone. The Cisco FXS interface is an RJ-11 connector that allows connections to basic telephone service equipment, keysets, and PBXs.

G

G.711 The 64-kbps PCM voice coding technique. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs. Described in the ITU-T standard in its G-series recommendations.

G.723.1 Compression technique that can be used for compressing speech or audio signal components at a very low bit rate as part of the H.324 family of standards. This codec has two bit rates associated with it: 5.3 and 6.3 kbps. The higher bit rate is based on ML-MLQ technology and provides a somewhat higher quality of sound. The lower bit rate is based on CELP and provides system designers with additional flexibility. Described in the ITU-T standard in its G-series recommendations.

G.729A CELP compression where voice is coded into 8-kbps streams. There are two variations of this standard (G.729 and G.729 Annex A) that differ mainly in computational complexity; both provide speech quality similar to 32-kbps ADPCM. Described in the ITU-T standard in its G-series recommendations.

GMT Greenwich Mean Time.

I

ICMP Internet Control Message Protocol. Network-layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

IETF Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards.

IP Internet Protocol. Network-layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.

ITU International Telecommunication Union. An organization established by the United Nations to set international telecommunications standards and to allocate frequencies for specific uses.

IVR Interactive voice response. Describes systems that provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words or, more commonly, DTMF signaling. Examples include banks that allow you to check your balance from any telephone and automated stock quote systems.

L

LDAP Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory.

LEC Local exchange carrier. A local telephone company or communications common carrier that provides ordinary local voice-grade telecommunications service under regulation within a specified service area.

location server A SIP redirect or proxy server uses a location server to get information about a caller's location. Location services are offered by location servers.

M

MCU Multipoint control unit. A bridging or switching device that supports multipoint videoconferencing.

MGCP Media Gateway Control Protocol.

MWI Message waiting indication.

mu-law Commonly written u-law. North American companding standard used in conversion between analog and digital signals in PCM systems. Similar to the European A-law. See also A-law and companding.

N

NAT Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into address space with global routing. Also known as Network Address Translator.

NTP Network Time Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

P

POTS Plain Old Telephone Service. Basic telephone service that supplies standard single-line telephones, telephone lines, and access to the PSTN.

proxy server An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets and, if necessary, rewrites a request message before forwarding it.

PSTN Public Switched Telephone Network. PSTN refers to the local telephone company.

Q

QoS Quality of service. The ability of a network, whether the network is a complex network, small corporate network, Internet service provider (ISP), or enterprise network, to provide better service to selected network traffic over various technologies, including Frame Relay, ATM, Ethernet and 802.1 networks, and SONET, as well as IP-routed networks that may use any or all of these underlying technologies.

R

RAS Registration, Admission, and Status Protocol. Protocol that is used between endpoints and a gatekeeper to perform management functions. RAS signalling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.

redirect server A server that accepts a SIP request, maps the address into zero or more new addresses, and returns these addresses to the client. It does not initiate its own SIP request nor accept calls.

registrar server A server that accepts REGISTER requests. A registrar is typically colocated with a proxy or redirect server and may offer location services.

RFC 2833 IETF standard that describes RTP payload for DTMF digits, telephony tones, and telephony signals.

router Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information. Occasionally called a gateway (although this definition of gateway is becoming increasingly outdated). Compare with gateway.

RSVP Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams that they want to receive. RSVP depends on IPv6. Also known as Resource Reservation Setup Protocol.

RTP Real-Time Transport Protocol. One of the IPv6 protocols. RTP is designed to provide end-to-end network transport functions for applications that transmit real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides services such as payload type identification, sequence numbering, time stamping, and delivery monitoring to real-time applications.

S

SCCP Skinny Call Control Protocol. A VoIP protocol utilized by a CallManager server.

SDP Session Definition Protocol. An IETF protocol for the definition of multimedia services. SDP messages can be part of SIP, MGCP, and SCCP and messages.

SIP Session Initiation Protocol. Protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.

SIP endpoint A terminal or gateway that acts as a source or sink of SIP voice data. An endpoint can call or be called, and it generates or terminates the information stream.

SLIC Subscriber Line Interface Circuit. An integrated circuit providing central office-like telephone interface functionality.

SNA Systems Network Architecture. Large, complex, feature-rich network architecture developed in the 1970s by IBM. Similar in some respects to the OSI reference model but with a number of differences. SNA essentially is composed of seven layers.

SOHO Small office, home office. Networking solutions and access technologies for offices that are not directly connected to large corporate networks.

T

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

TFTP Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

ToS Type of service. See CoS.

U

UAC User agent client. A client application that initiates the SIP request.

UAS User agent server (or user agent). A server application that contacts the user when a SIP request is received, and then returns a response on behalf of the user. The response accepts, rejects, or redirects the request.

UDP User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

u-law See mu-law.

V

VAD Voice activity detection. When enabled on a voice port or a dial peer, silence is not transmitted over the network, only audible speech. When VAD is enabled, the sound quality is slightly degraded but the connection monopolizes much less bandwidth.

VoIP Voice over IP. The capability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. VoIP is a blanket term, which generally refers to Cisco's standard-based approach to IP voice traffic.

X

XML eXtensible Markup Language. XML is an open standard for defining data elements on web pages and in business documents. See also BTXML.

Numerics

10/100 PC port 2-4
10/100 SW port 2-4
10 BASET port 2-4
802.1Q VLAN ID 3-5

A

AC adapter 2-5
ACK C-1
Admin. VLAN Id parameter 5-10
Alert-Info header 4-6
Allow Blind Transfer parameter 8-14
Allow Call Transfer parameter 8-14
Allow Call Waiting parameter 8-14
Allow Conference parameter 8-14
Alpha softkey 5-5
Alternate DNS parameter 5-13
Alternate Domain parameter 5-13
Alternate NTP parameter 5-13
Alternate TFTP parameter 5-12
AltNTPIP parameter 4-8, 8-6
AltProxyTimeOut parameter 8-10
anonymous calls, blocking 8-15, A-3
assistance, technical 9-5
attended call transfer A-3
AttendedTransfer parameter 8-14
AudioMode parameter 4-5, 8-25
audio parameters
  AudioMode 4-5, 8-25
  ConnectMode 4-8, 4-10, 8-26
  MediaPort 4-3, 4-7
  NumTxFrames 8-26
  RxCodec 8-25
  TOS 4-5
  TxCodec 8-25
Audio Parameters screen 8-24
authentication 4-4

B

Back softkey A-6
Backup Proxy Timeout parameter 5-16
basic services, list of supported 1-5
blind call transfer A-4, A-6
BlindTransfer parameter 8-14
BlndXfr softkey 8-14, A-6
Block Anonymous Calls parameter 8-15
BlockAnonymous parameter 8-15

Block Caller ID parameter 8-15
BlockCallerId parameter 8-15
bmp2logo.exe 8-44
boot load firmware image 2-9
boot load process 3-2
busy tone 8-23, 8-28, 9-3
BusyTone parameter 8-23, 8-28
BYE C-1

C

cable connections
  Cisco IP Phone 7905G 2-10
  Cisco IP Phone 7912G 2-11
caller ID
  blocking A-2, A-3
  display name 8-16, A-2
call forwarding 8-16, A-6
Call Forward Number parameter 8-16
CallForwardNumber parameter 8-16
call preference parameters
  Allow Blind Transfer 8-14
  Allow Call Transfer 8-14
  Allow Call Waiting 8-14
  Allow Conference 8-14
  AttendedTransfer 8-14
  BlindTransfer 8-14
  BlockAnonymous 8-15
  Block Anonymous Calls 8-15
  Block Caller ID 8-15
  BlockCallerId 8-15
  Call Forward Number 8-16
  CallForwardNumber 8-16
  CallPrefGuiSet 4-5, 8-20
  CallPrefGuiShow 4-5, 8-19
  CallWaiting 8-14
  Conference 8-14
  Date Format 8-17
  DateFormat 8-17, 8-18
  Display Name 8-16
  DisplayName 8-16
  Do Not Disturb 8-15
  DoNotDisturb 8-15
  Forward to VMail Delay 8-18
  GUI Set Mask 4-5, 8-20
  GUI Show Mask 4-5, 8-19
  Short Name 8-16
  ShortName 8-16
  Time Format 8-17
  TimeFormat 8-17
  Voice Mail Number 8-15
  VoiceMailNumber 8-15
Call Preferences menu
  allowing users to change parameters on 4-5, 8-20
  controlling parameters displayed on 4-5, 8-19
  customizing 4-5, 8-19, 8-20
  displaying A-2
  overview 5-2, A-1

parameters A-2 to A-6
Call Preferences menu parameters
Allow Blind Transfer A-4
Allow Call Transfer A-3
Allow Call Waiting A-3
Allow Conference A-4
Block Anonymous Call A-3
Block Caller ID A-3
Call Forward Number A-6
Date Format A-5
DisplayName A-2
Do Not Disturb A-3
Forward to VMail Delay(s) A-6
ShortName A-2
Time Format A-4
Voice Mail Number A-5
Call Preferences screen 8-13
CallPrefGuiSet parameter 4-5, 8-20
CallPrefGuiShow parameter 4-5, 8-19
call transfer
attended 8-14, A-3
blind 8-14, A-4, A-6
call waiting 8-14, A-3
CallWaiting parameter 8-14
call waiting tone 8-24, 8-28
CallWaitTone parameter 8-24, 8-28
CANCEL C-1
Cancel softkey 5-5
CDP
see Cisco Discovery Protocol
CDP Enabled parameter 5-11
cfgfmt.exe tool 6-9, 6-16
CfgInterval parameter 8-4
Cisco Discovery Protocol (CDP) 3-3, 3-4, 5-11, 8-7
Cisco IP Phone 7905G
electrical specifications D-2
environmental specifications D-3
graphic on LCD screen 8-27, 8-43
mounting to wall 2-12
physical interface specifications D-3
physical specifications D-2
port 2-4
resets repeatedly 9-4
software specifications D-3
Cisco IP Phone 7912G
electrical specifications D-2
environmental specifications D-3
graphic on LCD screen 8-27, 8-43
mounting to wall 2-12
physical interface specifications D-3
physical specifications D-2
ports 2-4
software specifications D-3
Clear softkey A-7
codec
number of text frames for 8-26
receiving 8-25

specification D-3
supported 1-5
transmitting 8-25
comfort noise 4-5
conference call 8-14, A-4
Conference parameter 8-14
configuration
alphabetical listing of features with related parameters 4-12
authentication 4-4
basic 2-13
cfgfmt.exe tool 6-16
dial plan 4-5
effecting changes 3-8
features and related parameters 4-12
from a Cisco IP Phone 5-4
individual phone 6-3
in TFTP server environment, basic steps 3-6 to 3-8
menus on phone 5-2
minimum settings for network connectivity 3-9
multiple phones 6-3
overview of methods 3-1
refresh interval 4-4, 8-4
required parameters 4-2
required SIP parameters 4-2 to 4-3
services and related parameters 4-12
silence suppression 4-5
SIP proxy server redundancy 4-10
TFTP server 3-1
through phone menus 3-2
through TFTP 6-2
tone 8-28
configuration file
see profile
configuration menu
displaying 5-3
entering parameter values 5-5
locking parameters 5-4
unlocking parameters 5-4
Confrn softkey 8-14, A-4
connecting, phone to network 2-4
ConnectMode parameter 4-8, 4-10, 8-26, 8-36

D

date format, on LCD screen 8-17, A-5
Date Format parameter 8-17
DateFormat parameter 8-17, 8-18
daylight savings time 5-9, 8-6, 9-3
debugging 4-5, 8-9, 9-5
default profile 6-13
default router IP address 5-8, 8-5
Default Router parameter 3-10, 5-8
Default softkey A-7
default values, setting parameters to 5-14
Device Information screen 7-4

DHCP
disabling 5-11, 8-4
enabling 5-11, 8-4
option 1 6-8
option 150 6-6, 8-7
option 3 6-8
option 42 6-8
option 6 6-8
option 60 6-7
option 66 6-6, 6-8
DHCP Enabled parameter 5-11
Dhcp parameter 8-4
DHCP server
configuration overview 3-2
configuration using 6-5, 6-8
configuration without using 3-3, 3-10, 6-8
IP address 5-6
DHCP Server parameter 5-6
diagnostics 4-5
dial plan
configuration 4-5
rules 8-13, 8-38
DialPlan parameter 4-5, 8-13, 8-38
dial tone 8-23, 8-28, 9-4
DialTone2 parameter 8-23, 8-28, 8-39
DialTone parameter 8-23, 8-28
direct IP-to-IP calls 4-10
display name, for caller ID 8-16, A-2
Display Name parameter 8-16
DisplayName parameter 8-16
distinctive ringing 4-6
DND softkey A-3, A-7
DNS
disabling alternate 5-13
enabling alternate 5-13
DNS1IP parameter 8-6
DNS2IP parameter 8-6
DNS server
IP address of primary 5-8, 8-6
IP address of secondary 5-8, 8-6
DNS Server 1 parameter 5-8
DNS Server 2 parameter 5-8
DNS SRV lookup 4-6
documentation, related xiii
domain name
disabling alternate 5-13
enabling alternate 5-13
of phone 8-5
Domain Name parameter 5-7
Domain parameter 8-5
Do Not Disturb 8-15, A-3, A-7
Do Not Disturb parameter 8-15
DoNotDisturb parameter 8-15
downloading, Cisco IP Phone software from CCO 6-4
Drop softkey A-7
DTMF transmission method 8-25

E

Edit softkey 5-6, 5-14
electrical specifications D-2
enabling SIP registration 4-2
encryption, of profile 6-15
encryption key 5-14, 8-4
EncryptKey parameter 6-15, 6-16, 8-4
environmental specifications D-3
Erase Configuration parameter 5-14

F

Factory softkey A-7
fast-busy tone 9-2
features, software 1-4
features and related parameters 4-12
firewall 9-2
firmware image
  .sbin extension 6-4, 8-42
  .zup extension 6-4, 8-42
  boot load 2-9
  installing on TFTP server 6-4
  signature for authentication 6-4, 8-42
  upgrading 3-6, 8-26, 8-41
Firmware Versions screen 5-18
Forward to VMail Delay parameter 8-18

G

gkdefault.cfg profile 3-7, 6-3, 6-13
graphic, on LCD screen 8-27, 8-43
GUI Set Mask parameter 4-5, 8-20
GUI Show Mask parameter 4-5, 8-19

H

handset 1-3
hardware overview 1-1
Hold button 1-3
Host Name parameter 5-6

I

Include parameter 3-7, 8-27
inline power 2-4, 2-5
installation
  configuration 2-13
  prerequisites 2-1
  procedure 2-6
  safety 2-2
  verifying 2-15
INVITE C-1
IP address
  default router 5-8, 8-5
  DHCP server 5-6
  network gateway 5-8

phone 5-7, 8-5
specifying manually 3-10
IP Address parameter 3-10, 5-7
IPDialPlan parameter 8-13

L

lddefault.cfg profile 3-4, 3-7, 6-3, 6-13
light strip, on handset 1-3
Local RTP Port parameter 4-3, 5-16
Local SIP Port parameter 4-3, 5-16
locking configuration parameters 5-4
log file 9-6
Login ID parameter 5-15
LoginID parameter 8-10
logo, on LCD screen 8-27, 8-43

M

MAC Address parameter 5-6
MAXRedirect parameter 4-2, 8-11
Media Access Control (MAC) address 5-6
media port 4-7
MediaPort parameter 4-3, 4-7, 8-12
menu
Call Preferences 5-2, A-1
Model Information 5-2, 5-17
Network Configuration 5-2, 5-6
SIP Configuration 5-2, 5-14
Status 5-2, 5-18
menu, displaying on phone 5-3
Menu button 1-3
message waiting A-8
Missed softkey A-7
Model Information menu 5-2, 5-17

N

name
displayed on LCD screen 8-16, A-2
for caller ID 8-16, A-2
NATIP parameter 4-3, 4-7, 8-11
NatServer parameter 4-8, 8-12
NatTimer parameter 4-8, 8-12
NAT WAN IP Address parameter 4-3, 5-17
Navigation button 1-3
network
connecting phone to 2-4
requirements for installation 2-1
Network Address Translation (NAT), overview 4-7
Network Address Translation (NAT) WAN, IP address 5-17, 8-11
Network Address Translation/Port Address Translation (NAT/PAT) 4-8
Network Configuration menu
overview 5-2
parameters 5-6 to 5-14
resetting parameters to default values 5-14

Network Configuration menu parameters
Admin. VLAN Id 5-10
Alternate DNS 5-13
Alternate Domain 5-13
Alternate NTP 5-13
Alternate TFTP 5-12
CDP Enabled 5-11
Default Router 3-10, 5-8
DHCP Enabled 5-11
DHCP Server 5-6
DNS Server 1 5-8
DNS Server 2 5-8
Domain Name 5-7
Erase Configuration 5-14
Host Name 5-6
IP Address 3-10, 5-7
MAC Address 5-6
NTP Server 1 5-9
NTP Server 2 5-9
Operational VLAN Id 5-10
Profile Encrypt Key 5-14
Subnet Mask 3-10, 5-7
TFTP Enabled 5-12
TFTP Server 5-8
Time Zone 5-9
VLAN Enabled 5-10
network connectivity, minimum settings 3-9
network gateway IP address 5-8
network parameters
AltNTPIP 4-8, 8-6
CfgInterval 8-4
Dhcp 8-4
DNS1IP 8-6
DNS2IP 8-6
Domain 8-5
EncryptKey 8-4
NPrintf 4-5, 8-9
NTPIP 4-8, 8-6
OpFlags 3-4, 6-17, 8-7
StaticIP 3-10, 8-5
StaticNetMask 3-10, 8-5
StaticRoute 3-10, 4-7, 8-5
TftpURL 8-3
TimeZone 4-8, 8-6
TOS 8-8
TraceFlags 4-5, 8-9
UseTftp 8-3
VLANSetting 3-5, 8-8
Network Parameters screen 8-2
Network Statistics screen 5-18
next hop server redundancy 4-9
No softkey 5-6, 5-14
NOTIFY C-1
NPrintf parameter 4-5, 8-9, 9-6
NTPIP parameter 4-8, 8-6
NTP server
address of primary 5-9
address of secondary 5-9

disabling alternate 5-13
enabling alternate 5-13
IP address of primary 8-6
IP address of secondary 8-6
NTP Server 1 parameter 5-9
NTP Server 2 parameter 5-9
Number softkey 5-5
NumTxFrames parameter 8-26

O

Operational VLAN Id parameter 5-10
OpFlags parameter 3-4, 6-17, 8-7
OPTIONS C-1
OutBoundProxy parameter 4-3, 8-12
Outbound Proxy parameter 4-3, 4-9, 5-16
outbound proxy server, address 4-3

P

padlock icon 5-4
parameters
audio 8-24 to 8-26
call preference 8-13 to 8-20
Call Preference menu A-2 to A-6
format in profile 6-10
in profile only 8-26 to 8-27
menu, web page, and profile equivalents B-1
network 8-2 to 8-9
Network Configuration menu 5-6 to 5-14
settings revert 9-2
SIP 8-9 to 8-13
SIP Configuration menu 5-15 to 5-17
tone 8-21 to 8-24
value types 6-11
parameter tag file 6-9, 6-13, 6-14
password 5-15, 8-10, 8-26
Password parameter 5-15
phone menu configuration 3-2
physical interface specifications D-3
physical specifications D-2
placing call without using SIP proxy 4-10
port
10/100 PC 2-4
10/100 SW 2-4
10 BASET 2-4
cable type for 2-4
for incoming SIP requests 4-3
media 4-7
power patch panel, providing power using 2-5
power source
description 2-5
design 2-5
external 2-5
inline power 2-5
power patch panel 2-5
redundancy 2-6
probing, of static network router 8-7

profile
about 2-7, 6-2
binary 6-9
common 6-13
conventions 6-10
creating 6-9
default 6-13
default values 6-11
defined 6-1
disabling downloading from TFTP server 5-12, 8-3
enabling downloading from TFTP server 5-12, 8-3
encrypting 6-15
example file 6-11
for individual phone 6-3
for multiple phones 6-3
gkdefault.cfg 3-7, 6-3
including parameters from another profile 8-27
IP address of TFTP server containing 8-3
lddefault.cfg 3-4, 3-7, 6-3
overwriting default name 8-7
phone-specific 6-11
SEPDefault.cnf 3-4
text 6-10
updating 6-9
XMLDefault.cnf.xml 3-4
Profile Encrypt Key parameter 5-14
protocols
list of supported 1-4
SIP overview 1-7
specification D-3
Proxy parameter 4-3, 4-9, 8-10
proxy redundancy 4-9
proxy server 1-10
prserv.exe 9-5, 9-6
ptag.dat 6-9
PWD parameter 8-10

R

ready screen, on phone 2-9, 9-3
redirection, maximum number of times to try 4-2
redirect server 1-10
redundancy, for power 2-6
refreshing
Cisco IP Phone 6-17
disabling 8-7
enabling 8-7
refresh interval, configuration 3-8, 4-4, 8-4
REGISTER C-1
Register Expires parameter 4-2, 5-17
Register with Proxy parameter 4-2, 5-17
registrar server 1-10
registration
with authentication C-4
without authentication C-2

registration renewal, configuring seconds between 4-2, 5-17, 8-11
registration status icon 8-19
related documentation xiii
reorder tone 8-24, 8-30
ReorderTone parameter 8-24, 8-30
required parameters, description of 4-2
resetting
  Cisco IP Phone 6-17
  disabling 8-7
  enabling 8-7
Restore softkey A-7
ring back tone 8-24, 8-28
RingBackTone parameter 8-24, 8-28
ringer cadence pattern 8-23
ringer sound A-8
ringing, distinctive 4-6
RingOnOffTime parameter 8-23
router IP address, specifying manually 3-10
RTP media port 4-3
RxCodec parameter 8-25

S

sample configuration text file 6-11
Save softkey 5-5
screens
  Audio Parameters 8-24
  Call Preferences 8-13
  Device Information 7-4
  Network Parameters 8-2
  SIP Parameters 8-9
secondary dial tone 8-28
SEPDefault.cnf profile 3-4
services
  basic 1-5
  related parameters 4-12
  SIP, list of supported 1-6
  supplemental, list of supported 1-5
Short Name parameter 8-16
ShortName parameter 8-16
signal events, timeout values 8-22
SigTimer parameter 8-22
silence suppression 4-5, 8-25
SIP
  call flow scenarios C-2
  clients 1-9
  components 1-8
  functions 1-7
  overview 1-7
  request methods C-1
  responses C-2
  servers 1-10
sip_ptag.dat 6-10
SIP Configuration menu
  overview 5-2
  parameters 5-14 to 5-17
  resetting parameters to default values 5-14

SIP Configuration menu parameters
Backup Proxy Timeout 5-16
Local RTP Port 4-3, 5-16
Local SIP Port 4-3, 5-16
Login ID 5-15
NAT WAN IP Address 4-3, 5-17
Outbound Proxy 4-3, 4-9, 5-16
Password 5-15
Register Expires 4-2, 5-17
Register with Proxy 4-2, 5-17
SIP Proxy 4-3, 5-15
Use Login ID 5-15
User ID 5-15
sipexample.txt sample configuration file 6-11
SIP outbound proxy server, IP address 5-16, 8-12
SIP parameters
AltProxyTimeOut 8-10
DialPlan 8-13
IPDialPlan 8-13
LoginID 8-10
MAXRedirect 4-2, 8-11
MediaPort 8-12
NATIP 4-7, 8-11
NatServer 4-8, 8-12
NatTimer 4-8, 8-12
OutBoundProxy 4-3, 8-12
Proxy 4-3, 4-9, 8-10
PWD 8-10
SIPPort 4-3, 4-7, 8-11
SIPRegInterval 4-2, 8-11
SIPRegOn 8-11
UID 8-10
UseLoginID 4-4, 8-10
SIP Parameters screen 8-9
SIPPort parameter 4-3, 4-7, 8-11
SIP proxy not used for call 4-10
SIP Proxy parameter 4-3, 5-15
SIP proxy server
IP address 4-3, 5-15, 8-10
redundancy 4-10
SIPRegInterval parameter 4-2, 8-11
SIP registration
disabling 5-17, 8-11
enabling 4-2, 5-17, 8-11
SIPRegOn parameter 4-2, 8-11
SIP services
advanced 4-4
basic 4-2
list of supported 1-6
SIP to SIP call
with authentication C-15
without authentication C-7
softkey
Back A-6
back 5-3
BlndXfr A-6
Cancel 5-5
Clear A-7

Default A-7
DND A-7
Drop A-7
Edit 5-6, 5-14
Exit 5-3
Factory A-7
Missed A-7
No 5-6, 5-14
Restore A-7
Save 5-5
Validate 5-5
Yes 5-6, 5-14
software
downloading from CCO 6-4
overview 1-4
protocols, list of supported 1-4
software specifications D-3
specifications
electrical D-2
environmental D-3
physical D-2
physical interface D-3
software D-3
startup process, of phone 2-9
StaticIP parameter 3-10, 8-5
StaticNetMask parameter 3-10, 8-5
StaticRoute parameter 3-10, 4-7, 8-5
Status menu 5-2, 5-18
Status Messages screen 5-18
stutter tone A-8
subnet mask
specifying manually 3-10
used by phone 5-7, 8-5
Subnet Mask parameter 3-10, 5-7
subscription features 4-5
supplemental services, list of supported 1-5

T

TAC, contacting 9-5
tag, length, and value triplets 6-2
technical assistance 9-5
TFTP
configuration, about 6-2
disabling 5-12
disabling alternate server 5-12
enabling 5-12
enabling alternate server 5-12
server configuration
overview 3-1
TFTP Enabled parameter 5-12
TFTP server
configuration overview 3-1
disabling downloading of profile from 5-12, 8-3
enabling downloading of profile from 5-12, 8-3
IP address 5-8, 6-6, 8-3
name 6-6

URL 5-8
TFTP Server parameter 5-8
TftpURL parameter 8-3
time, display 9-3
time format, on LCD screen 8-17, A-4
Time Format parameter 8-17
TimeFormat parameter 8-17
time zone, of time on phone 5-9, 8-6
Time Zone parameter 5-9
TimeZone parameter 4-8, 8-6
tone
busy tone 8-23, 8-28
cadences in 8-28
call waiting tone 8-24, 8-28
configuration 8-28
dial tone 8-23, 8-28, 9-4
fast busy tone 9-2, 9-3
frequencies in 8-28
reorder 8-24, 8-30
ring back tone 8-24, 8-28
secondary dial tone 8-23, 8-28
tone parameters
BusyTone 8-23
CallWaitTone 8-24
DialPlan 4-5
DialTone 8-23
DialTone2 8-23
ReorderTone 8-24
RingBackTone 8-24
RingOnOffTime 8-23
SigTimer 8-22
ToS (Type of Service) 8-8
TOS parameter 4-5, 8-8
TraceFlags parameter 4-5, 8-9
Trnsfer softkey 8-14
troubleshooting
contacting TAC 9-5
general tips 9-1
resolving problems 9-2
TxCodec parameter 8-25

U

UID parameter 8-10
UIPassword parameter 8-26
unlocking configuration parameters 5-4
upgradecode parameter 3-7, 8-26, 8-41
upgradelogo parameter 8-27, 8-45
Use Login ID parameter 5-15
UseLoginID parameter 4-4, 8-10
user-agent client (UAC) 1-8
user-agent server (UAS) 1-8
user ID 5-15, 8-10
User ID parameter 5-15
UseTftp parameter 8-3

V

Validate softkey 5-5
VLAN
  auxiliary 5-10
  disabling 5-10
  enabling 5-10
  IP encapsulation, disabling 8-7
  IP encapsulation, enabling 8-7
  related parameters 3-4
  tagging 3-3
  use of 8-8
VLAN CoS bit value
  specifying for TCP packets 3-5
  specifying for UDP packets 3-5
VLAN Enabled parameter 5-10
VLAN ID
  enabling user-specified voice 3-4
  example 3-5
  specifying a preconfigured 3-4
VLAN IP encapsulation
  disabling 3-4
VLAN IP encapsulation, disabling 3-4
VLANSetting parameter 3-5, 8-8
Voice Mail Number parameter 8-15
VoiceMailNumber parameter 8-15
voice messages 8-15, A-5
voice message system
  delay before call is forwarded to 8-18, A-6
  phone number for 8-15, A-5
Volume button 1-3

W

wall mounting, Cisco IP Phone 2-12
WAN, address of attached router/NAT 4-3
warnings
  connecting SELV circuits to TNV circuits 2-8
  connecting to power source 2-3
  disposal 2-2
  installation by service personnel only 2-3
  lightning 2-3
  plug-socket combination 2-3
  short-circuit (overcurrent) protection 2-3
  TN power systems 2-3
web page
  accessing for a phone 7-2
  Audio Parameters 8-24
  Call Preferences 8-13
  configuration options 7-3
  configuring 7-2
  Device Information 7-4
  disabling access to 4-5
  for Cisco IP Phone 7905G 7-1, 7-2
  for Cisco IP Phone 7912G 7-1, 7-2
  Network Parameters 8-2
  password 7-4
  SIP Parameters 8-9

X

XMLDefault.cnf.xml profile **3-4**

Y

Yes softkey **5-6, 5-14**